



Palo Alto Networks®

Guía de implementación de la serie VM
PAN-OS 6.0

Información de contacto

Sede de la empresa:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Acerca de esta guía

Esta guía describe cómo configurar y obtener una licencia para el cortafuegos de la serie VM, y está dirigida a administradores que deseen implementar el cortafuegos de la serie VM.

Para obtener más información, consulte las siguientes fuentes:

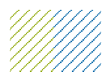
- Guía del administrador de PAN-OS: para obtener instrucciones sobre cómo configurar las funciones del cortafuegos.
- https://paloaltonetworks.com/documentation: para acceder a bases de conocimientos, a un completo conjunto de documentación, foros de discusión y vídeos.
- https://support.paloaltonetworks.com: para ponerse en contacto con el equipo de asistencia técnica, obtener información sobre los programas de asistencia técnica o gestionar la cuenta o los dispositivos.
- Si desea las notas de versión más recientes, vaya a la página de descargas de software en https://support.paloaltonetworks.com/Updates/SoftwareUpdates.

Para enviar sus comentarios sobre la documentación, diríjase a: documentation@paloaltonetworks.com.

Palo Alto Networks, Inc.
www.paloaltonetworks.com

28 de marzo de 2014

Contenido



Acerca del cortafuegos de la serie VM

El cortafuegos de la serie VM de Palo Alto Networks es la versión virtualizada de cortafuegos de última generación de Palo Alto Networks. Es ideal para su uso en un entorno de centro de datos virtualizado donde puede proteger y asegurar el tráfico para implementaciones de la nube pública y privada.

Modelos de la serie VM

El cortafuegos de la serie VM está disponible en cuatro modelos (VM-100, VM-200, VM-300 y VM-1000-HV).

Los cuatro modelos pueden implementarse como máquinas virtuales invitadas en ESXi de VMware y NetScaler SDX de Citrix; en NSX de VMWare solo se admite VM-1000-HV. El paquete de software (archivo *.xva* o *.ovf*) que se usa para implementar el cortafuegos de la serie VM es común en todos los modelos. El modelo de la serie VM funciona con licencia; cuando aplica la licencia en el cortafuegos de la serie VM, el número de modelo y las capacidades asociadas se implementan en el cortafuegos.

Cada modelo puede adquirirse en versión Individual o Enterprise. La versión Individual se vende por unidades. El SKU que solicite, por ejemplo PA-VM-300, incluye un código de autenticación para obtener licencia de una instancia del cortafuegos de la serie VM. La versión Enterprise está disponible en bloques de 25 unidades. Por ejemplo, el SKU de pedido PAN-VM-100-ENT tiene un único código de autenticación que le permite registrar 100 instancias del VM-100.

Cada modelo de cortafuegos de la serie VM tiene licencia para una capacidad máxima. La capacidad se define por el número de sesiones, reglas, zonas de seguridad, objetos de dirección, túneles VPN de IPSec y túneles VPN SSL que el cortafuegos de la serie VM está optimizado para gestionar. Al adquirir una licencia, asegúrese de que adquiere la licencia correcta basándose en sus requisitos de red. La siguiente tabla describe algunas de las diferencias de capacidad por modelo:

Modelo	Sesiones	Reglas de seguridad	Direcciones IP dinámicas	Zonas de seguridad	Túneles de VPN IPSec	Túneles de VPN SSL
VM-100	50000	250	1000	10	25	25
VM-200	100000	2000	1000	20	500	200
VM-300	250000	5000	1000	40	2000	500
VM-1000-HV	250000	10000	100000	40	2000	500

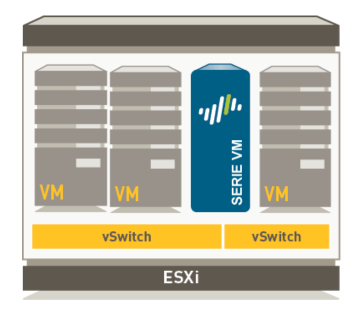
Implementaciones de la serie VM

El cortafuegos de la serie VM puede implementarse en las siguientes plataformas:

❒ Serie VM para el hipervisor vSphere de VMware (ESXi)

VM-100, VM-200, VM-300 o VM-1000-HV se implementan como máquina virtual invitada en ESXi de VMware; ideal para redes o nubes en las que es necesaria una versión virtual.

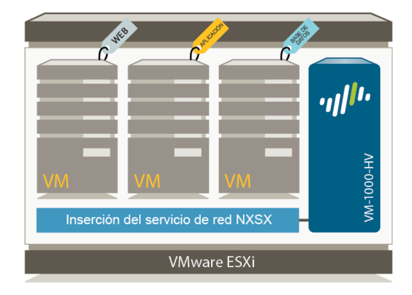
Para obtener más información, consulte Configuración de un Cortafuegos de la serie VM en un servidor ESXi.



❒ Serie VM para NSX de VMware

El modelo VM-1000-HV se implementa como un servicio de introspección de red con NSX de VMware y Panorama. Esta implementación es ideal para la inspección del tráfico horizontal.

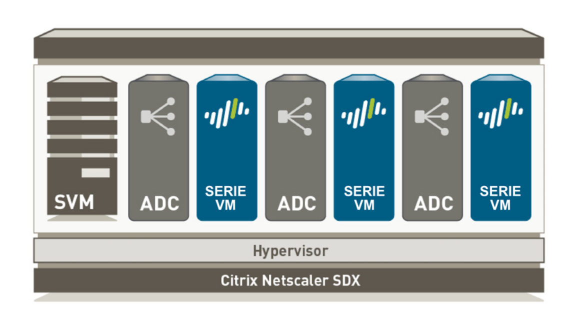
Si desea información detallada, consulte Cortafuegos de la edición NSX de la serie VM



❒ Serie VM para SDX de Citrix

VM-100, VM-200, VM-300 o VM-1000-HV se implementan como máquina virtual invitada en NetScaler SDX de Citrix; consolida los servicios de seguridad y ADC y las implementaciones de XenApp/XenDesktop de Citrix.

Si desea información detallada, consulte Configuración de un Cortafuegos de la serie VM en el servidor Citrix SDX



Obtención de licencia del Cortafuegos de la serie VM

Cuando adquiere un cortafuegos de la serie VM recibe un conjunto de códigos de autenticación por correo electrónico. Por lo general en el correo se incluye un código de autenticación de capacidad para el modelo adquirido (VM-100, VM-200, VM300, VM-1000-HV), un código de autenticación de asistencia técnica y software (por ejemplo el código de autenticación del SKU PAN-SVC-PREM-VM-100) que proporciona acceso a las actualizaciones de software/contenido y a la asistencia técnica. Si adquiere suscripciones adicionales para la prevención de amenazas, el filtrado URL, GlobalProtect o WildFire, se incluye una lista de los otros códigos de autenticación adquiridos con el pedido.

Si aún no dispone de una cuenta de asistencia técnica, deberá usar el código de autenticación de capacidad para registrar y crear una cuenta en el portal de asistencia. Una vez se verifique su cuenta y finalice el registro, podrá iniciar sesión y descargar el paquete de software necesario para instalar el cortafuegos de la serie VM. Si ya tiene una cuenta de asistencia técnica, puede acceder al enlace **Código de autenticación de la serie VM** de la página de software de asistencia técnica para gestionar sus licencias del cortafuegos de la serie VM y descargar el software.



Si tiene una copia de evaluación del cortafuegos de la serie VM y desea convertirlo en una copia con licencia completa (adquirida), clone su cortafuegos de la serie VM y use las instrucciones para registrar y asignar una licencia a la copia adquirida de su cortafuegos de la serie VM. Para obtener instrucciones, consulte Actualización del modelo de la serie VM.

Para adquirir una licencia para su cortafuegos de la serie VM, consulte las siguientes secciones:

- Creación de una cuenta de asistencia técnica
- Registro del cortafuegos de la serie VM
- Activación de la licencia
- Actualización de la versión de software de PAN-OS
- Actualización del modelo de la serie VM

Si desea instrucciones sobre la instalación de su cortafuegos de la serie VM, consulte Implementaciones de la serie VM.

Creación de una cuenta de asistencia técnica

Se necesita una cuenta de asistencia técnica para gestionar sus licencias del cortafuegos de la serie VM y descargar el paquete de software necesario para instalar el cortafuegos de la serie VM. Si ya tiene una cuenta de asistencia técnica, continúe con Registro del cortafuegos de la serie VM.

Creación de una cuenta de asistencia técnica
1. Inicie sesión en https://support.paloaltonetworks.com/.
2. Haga clic en **Registrar** y cumplimente los detalles en el formulario de registro de usuarios. Debe usar el código de autenticación de capacidad y el número de pedido de compra o venta para registrar y crear una cuenta en el portal de asistencia técnica.
3. **Envíe** el formulario. Recibirá un correo electrónico con un vínculo para activar la cuenta de usuario; complete los pasos para activar la cuenta. Una vez se verifique su cuenta y finalice el registro, podrá iniciar sesión y descargar el paquete de software necesario para instalar el cortafuegos de la serie VM.

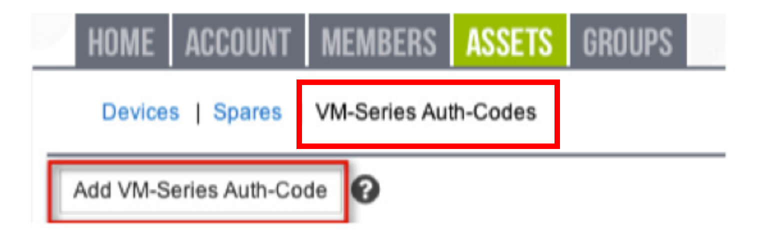
Registro del cortafuegos de la serie VM

Siga las instrucciones de esta sección para registrar su código de autenticación de capacidad con su cuenta de asistencia técnica.

Registro del cortafuegos de la serie VM

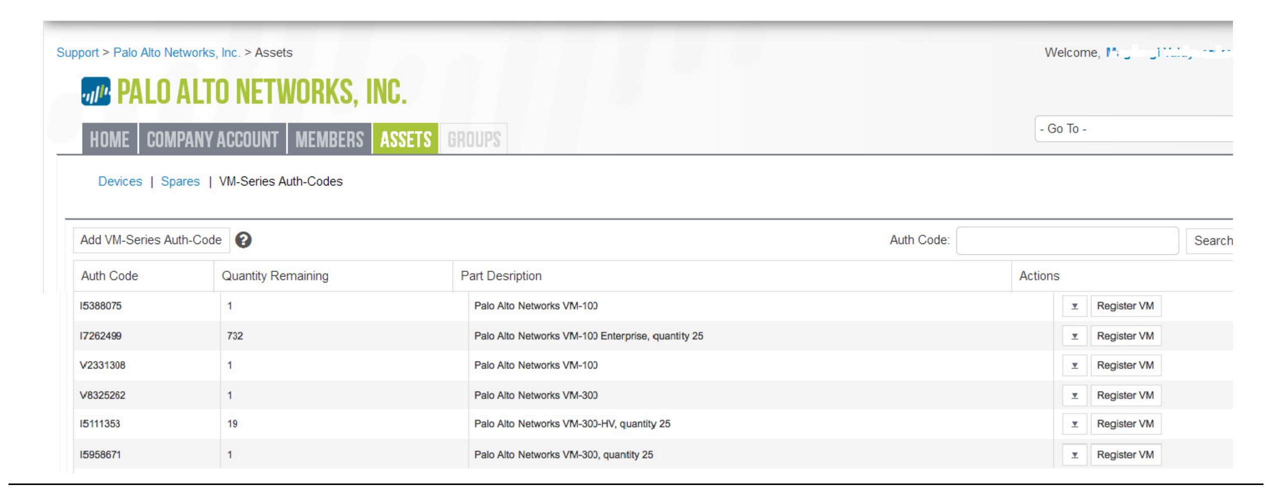
1. Inicie sesión en https://support.paloaltonetworks.com con sus credenciales de cuenta.

2. Seleccione **Activos** y haga clic en **Añadir códigos de autenticación de la serie VM.**



3. En el campo **Añadir códigos de autenticación de la serie VM**, introduzca el código de autenticación de capacidad que recibió por correo electrónico y haga clic en la marca de verificación para guardar lo que ha introducido. La página mostrará la lista de códigos de autenticación registrados en su cuenta de asistencia técnica.

   Puede hacer un seguimiento del número de cortafuegos de la serie VM que se han implementado y el número de licencias que siguen disponibles con cada código de autenticación. Cuando se hayan usado todas las licencias disponibles, el código de autenticación dejará de aparecer en la página Códigos de autenticación de la serie VM. Para ver todos los activos que se han implementado, seleccione **Activos > Dispositivos**.



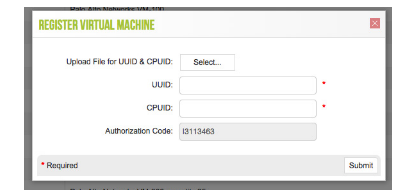
Auth Code	Quantity Remaining	Part Desription	Actions
I5388075	1	Palo Alto Networks VM-100	Register VM
I7262499	732	Palo Alto Networks VM-100 Enterprise, quantity 25	Register VM
V2331308	1	Palo Alto Networks VM-100	Register VM
V8325262	1	Palo Alto Networks VM-300	Register VM
I5111353	19	Palo Alto Networks VM-300-HV, quantity 25	Register VM
I5958671	1	Palo Alto Networks VM-300, quantity 25	Register VM

Activación de la licencia

Para activar la licencia en su cortafuegos de la serie VM, deberá haber implementado el cortafuegos de la serie VM y haber completado la configuración inicial. Si desea instrucciones sobre la implementación del cortafuegos de la serie VM, consulte Implementaciones de la serie VM.

Hasta que haya activado la licencia en el cortafuegos de la serie VM, el cortafuegos no tendrá un número de serie, la dirección MAC de las interfaces del plano de datos no serán únicas y solo se admitirá un número mínimo de sesiones. Como las direcciones MAC no son únicas hasta que el cortafuegos recibe licencia, para evitar problemas por superposición de direcciones MAC asegúrese de no tener múltiples cortafuegos de la serie VM sin licencia.

Cuando activa la licencia, el servidor de licencias usa la UUID y la Id. de la CPU de la máquina virtual para generar un número de serie único para el cortafuegos de la serie VM. El código de autenticación de capacidad, junto con el número de serie, se usa para validar su autorización.

Activación de la licencia	
• Si su cortafuegos de la serie VM tiene acceso directo a Internet.	1. Seleccione **Dispositivo > Licencias** y seleccione el vínculo **Activar función usando el código de autenticación**. 2. Introduzca el código de autenticación de capacidad que registró en el portal de asistencia técnica. El cortafuegos se conectará con el servidor de actualización (updates.paloaltonetworks.com), descargará la licencia y se reiniciará automáticamente. 3. Vuelva a iniciar sesión en la interfaz web y confirme que el **Panel** muestra un número de serie válido. Si aparece el término *Desconocido*, significa que el dispositivo no tiene licencia. 4. En **Dispositivo > Licencias**, compruebe que se añade la licencia **PA-VM** al dispositivo.
• Si su cortafuegos de la serie VM tiene acceso directo a Internet.  	1. Desplácese hasta **Dispositivo > Licencias** y haga clic en el vínculo **Activar función usando el código de autenticación**. 2. Haga clic en **Descargar archivo de autorización** y descargue *authorizationfile.txt* en la máquina cliente. 3. Copie *authorizationfile.txt* en un ordenador que tenga acceso a Internet e inicie sesión en el portal de asistencia técnica. Haga clic en el vínculo **Mis códigos de autenticación de la serie VM** y seleccione el código de autenticación aplicable en la lista y haga clic en el vínculo **Registrar VM**. 4. Cargue el archivo de autorización en la ficha **Registrar máquina virtual**. Esto completará el proceso de registro y el número de serie y el cortafuegos de la serie VM se añadirá a sus registros de cuenta. 5. Desplácese hasta **Activos > Mis dispositivos**, busque el dispositivo de la serie VM que acaba de registrar y haga clic en el vínculo **PA-VM**. Esto descargará la clave de licencia de la serie VM en la máquina cliente. 6. Copie la clave de licencia en la máquina que puede acceder a la interfaz web del cortafuegos de la serie VM y desplácese hasta **Dispositivo > Licencias**. 7. Haga clic en **Clave de licencia de carga manual** e introduzca la clave de licencia. Cuando la licencia de capacidad se haya activado en el cortafuegos se producirá el reinicio. 8. Inicie sesión en el dispositivo y confirme que el **Panel** muestra un número de serie válido y que la licencia muestra **PA-VM** en la ficha **Dispositivo > Licencias**.

Actualización de la versión de software de PAN-OS

Ahora que el cortafuegos de la serie VM tiene conectividad de red y el software PAN-OS básico está instalado, deberá actualizarlo a la versión más reciente de PAN-OS (se requiere una licencia de asistencia técnica).

Actualización de la versión de PAN-OS
1. Desde la interfaz web, desplácese hasta **Dispositivo > Licencias** y asegúrese de que tiene la licencia correcta para el cortafuegos de la serie VM y que la licencia está activada.
2. Para actualizar el software PAN-OS del cortafuegos de la serie VM, desplácese hasta **Dispositivo > Software**.
3. Haga clic en **Actualizar** para ver la versión de software más reciente; asimismo, revise **Notas de versión** para ver una descripción de los cambios de una versión y la ruta de migración para instalar el software.
4. Haga clic en **Descargar** para recuperar el software y, a continuación, haga clic en **Instalar**.

Actualización del modelo de la serie VM

El proceso de licencia del cortafuegos de la serie usa la UUID y la Id. de CPU para generar un número de serie único para cada cortafuegos de la serie VM. Así, cuando genera una licencia, esta se asigna a una instancia específica del cortafuegos de la serie VM y no puede modificarse.

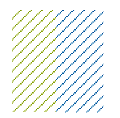
Para aplicar una nueva licencia de capacidad a un cortafuegos que se haya licenciado anteriormente, deberá clonar el cortafuegos existente (totalmente configurado) de la serie VM y aplicar una nueva licencia a la instancia clonada del cortafuegos.

Use las instrucciones de la sección si está:

- Migrando desde una licencia de evaluación a otra de producción.
- Actualizando el modelo para permitir una mayor capacidad. Por ejemplo, si desea actualizar del VM-200 a la licencia de VM-1000-HV.

Migración de la licencia del cortafuegos de la serie VM		
Paso 1	Desactive el cortafuegos de la serie VM.	
Paso 2	Clone el cortafuegos de la serie VM.	Si está clonando de forma manual, cuando se le pregunte indique que está copiando el cortafuegos, no moviéndolo.
Paso 3	Encienda la nueva instancia del cortafuegos de la serie VM.	1. Inicie la consola de número de serie del cortafuegos en la interfaz web de vSphere/SDX e introduzca el siguiente comando: `show system info` 2. Compruebe que: • el número de serie es desconocido • el cortafuegos no tiene licencias • la configuración está intacta

Migración de la licencia del cortafuegos de la serie VM		
Paso 4	Registre el nuevo código de autenticación en el portal de asistencia.	Consulte Registro del cortafuegos de la serie VM.
Paso 5	Aplique la nueva licencia.	Consulte Activación de la licencia.



Configuración de un Cortafuegos de la serie VM en un servidor ESXi

El cortafuegos de la serie VM se distribuye mediante el formato abierto de virtualización (OVF), que es un método estándar de empaquetar e implementar máquinas virtuales. Puede instalar esta solución en cualquier dispositivo x86 capaz de ejecutar VMware ESXi.

Para implementar un cortafuegos de la serie VM debe estar familiarizado con VMware y vSphere, incluidas las redes vSphere, la instalación y configuración de host ESXi y la implementación de máquinas virtuales invitadas.

Si desea automatizar el proceso de implementación de un cortafuegos de la serie VM, puede crear una plantilla estándar de referencia con la configuración y políticas óptimas y usar la API de vSphere y la API XML de PAN-OS para implementar rápidamente nuevos cortafuegos de la serie VM en su red. Para obtener detalles, consulte el artículo: Automatización del centro de datos de la serie VM.

Consulte los siguientes temas si desea información sobre:

- ▲ Implementaciones compatibles
- ▲ Requisitos y limitaciones del sistema
- ▲ Instalación de un cortafuegos de la serie VM
- ▲ Solución de problemas de implementaciones de ESXi

Implementaciones compatibles

Puede implementar una o varias instancias del cortafuegos de la serie VM en el servidor ESXi. La ubicación del cortafuegos de la serie VM en la red dependerá de su topología. Seleccione una de las siguientes opciones:

- **Un cortafuegos de la serie VM por host ESXi**: todos los servidores VM del host ESXi atraviesan el cortafuegos antes de salir del host por la red física. Los servidores VM se adjuntan al cortafuegos a través de los conmutadores estándar virtuales. Los servidores invitados no tienen ninguna otra conectividad de red, por lo que el cortafuegos visualiza y controla todo el tráfico que sale del host ESXi. Una variación de este caso de uso es también exigir que todo el tráfico fluya por el cortafuegos, incluyendo el tráfico de servidor a servidor (tráfico horizontal) en el mismo host ESXi.
- **Un cortafuegos de la serie VM por red virtual**: implemente un cortafuegos de la serie VM para cada red virtual. Si ha diseñado su red de modo que uno o más hosts ESXi tengan un grupo de máquinas virtuales que pertenezcan a la red interna, un grupo que pertenezca a la red externa y otros a la DMZ; puede implementar un cortafuegos de la serie XM para salvaguardar los servidores de cada grupo. Si un grupo o red virtual no comparte un conmutador virtual o grupo de puertos con otra red virtual, estará totalmente aislado de las demás redes virtuales del host. Como no hay otra ruta física o virtual a ninguna otra red, los servidores de cada red virtual deben usar el cortafuegos para comunicarse con cualquier otra red. Esto ofrece al cortafuegos visibilidad y control sobre todo el tráfico que abandona el conmutador virtual (estándar o distribuido) adjunto a cada red virtual.
- **Entorno híbrido**: se usan tanto host físicos como virtuales, el cortafuegos de la serie VM puede implementarse en una ubicación de agregación tradicional en lugar de un dispositivo de cortafuegos físico para conseguir los beneficios de una plataforma de servidor común para todos los dispositivos y para desvincular las dependencias de actualización de hardware y software.

Requisitos y limitaciones del sistema

Esta sección enumera los requisitos y las limitaciones del cortafuegos de la serie VM.

Requisitos

Puede crear e implementar una o varias instancias del cortafuegos de la serie VM en el servidor ESXi. Como todas las instancias del cortafuegos necesitan una asignación de recursos mínima (cantidad de CPU, memoria y espacio en disco) en el servidor ESXi, asegúrese de cumplir las especificaciones que aparecen a continuación para garantizar un rendimiento óptimo.

El cortafuegos de la serie VM tiene los siguientes requisitos:

- VMware ESXi con vSphere 4.1 y 5.0 para la serie VM que ejecute PAN-OS 5.0; VMware ESXi con vSphere 5.5 para la serie VM que ejecute PAN-OS 6.0.
- Un mínimo de dos vCPU por cada cortafuegos de la serie VM. Una para el plano de gestión y la otra para el plano de datos.

  Puede asignar 2 o 6 vCPU adicionales para asignar un total de 2, 4 u 8 vCPU al cortafuegos; el plano de gestión solo usa una vCPU y puede asignar las vCPU adicionales al plano de datos.
- Un mínimo de dos interfaces de red (vmNIC). Una será una vmNIC específica para la interfaz de gestión y la otra para la interfaz de datos. A continuación, podrá añadir hasta ocho vmNIC más para el tráfico de datos.

  El cortafuegos de la serie VM requiere que el modo promiscuo se defina como “aceptar” en el grupo de puertos del conmutador virtual en el que se adjuntan las interfaces de datos del cortafuegos.
- Un mínimo de 4 GB de memoria para todos los modelos excepto el VM-1000-HV, que necesita 5 GB. Cualquier memoria adicional se utilizará únicamente en el plano de gestión. Si está aplicando la licencia VM-1000-HV, consulte ¿Cómo puedo modificar el archivo de imagen base de la licencia de VM-1000-HV?
- Un mínimo de 40 GB de espacio de disco virtual. Puede añadir un disco adicional de hasta 2 TB para su registro.

Limitaciones

Las prestaciones del cortafuegos de la serie VM son muy parecidas a las de los cortafuegos de hardware de Palo Alto Networks, pero con las siguientes limitaciones:

- Se requieren núcleos CPU dedicados.
- Únicamente se admite la versión lite de alta disponibilidad (HA) (activo/pasivo sin conmutación por error con estado).
- La supervisión de enlaces de alta disponibilidad (HA) únicamente se admite en instalaciones de VMware ESXi que admitan E/S de DirectPath.
- Es posible configurar hasta 10 puertos en total; esta es una limitación de VMware. Se utilizará uno para el tráfico de gestión y hasta 9 para el tráfico de datos.

- Únicamente se admite el controlador vmxnet3.
- Los sistemas virtuales no son compatibles.
- No se admite vMotion.
- No se admiten tramas gigantes.
- No se admite la agregación de enlaces.

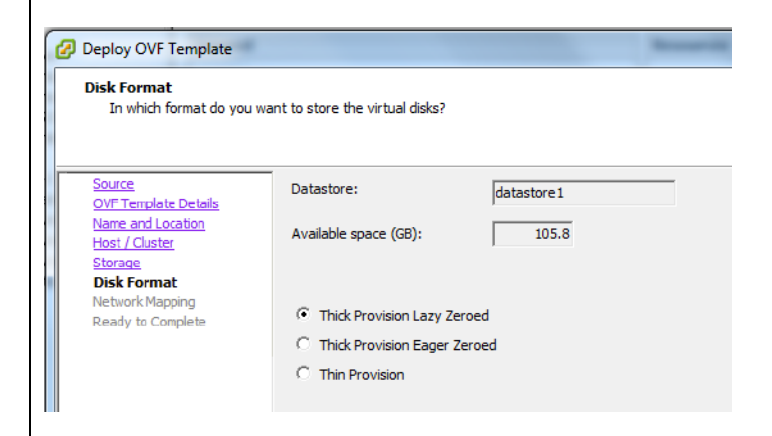
Instalación de un cortafuegos de la serie VM

Para instalar un cortafuegos de la serie VM debe tener acceso a la plantilla de formato abierto de virtualización (OVF). Use el código de autenticación que recibió con el correo electrónico de cumplimentación del pedido para registrar su cortafuegos de la serie VM y recuperar el acceso a la plantilla de OVF. El OVF se descarga como archivo comprimido zip que se expande en tres archivos: la extensión .ovf es para el archivo descriptor OVF que contiene todos los metadatos del paquete y su contenido; la extensión .mf es para el archivo de manifiesto OVF que contiene los resúmenes SHA-1 de los archivos individuales del paquete, y la extensión .vmdk se aplica al archivo de imagen de disco virtual que contiene la versión virtualizada del cortafuegos.

- Aprovisionamiento del cortafuegos de la serie VM
- Realización de la configuración inicial

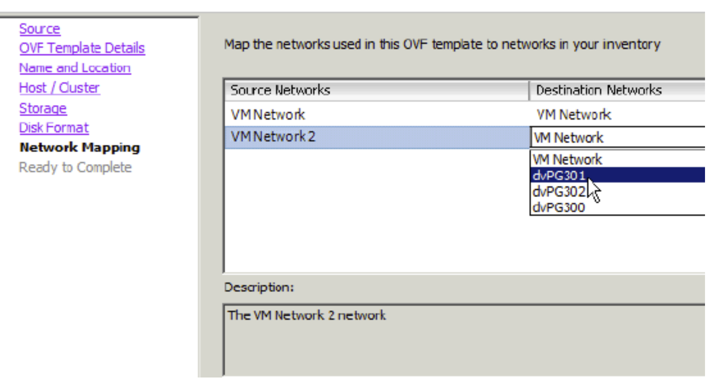
Aprovisionamiento del cortafuegos de la serie VM

Aprovisionamiento del cortafuegos de la serie VM		
Paso 1	Descargue el archivo zip que contiene la plantilla de OVF.	Registre su cortafuegos de la serie VM y obtenga la plantilla de OVF de: https://support.paloaltonetworks.com . **Nota** Los archivos anteriores contienen la instalación básica. Cuando la instalación básica haya finalizado, deberá descargar e instalar la versión más reciente de PAN-OS desde el sitio web de asistencia técnica. Con ello garantizará que cuenta con los ajustes más recientes implementados desde la creación de la imagen básica. Para obtener instrucciones, consulte Actualización de la versión de software de PAN-OS.
Paso 2	Antes de implementar la plantilla de OVF, configure los conmutadores estándar virtuales y conmutadores distribuidos virtuales que necesitará para el cortafuegos de la serie VM. **Nota** El cortafuegos de la serie VM requiere que todos los conmutadores virtuales conectados tengan habilitado el modo promiscuo.	**Para configurar un conmutador estándar virtual para el modo promiscuo:** 1. Configure un conmutador estándar virtual desde el cliente vSphere desplazándose hasta **Inicio > Inventario > Hosts y clústeres**. 2. Haga clic en la ficha **Configuración** y, bajo **Hardware**, haga clic en **Redes**. Para cada conmutador virtual conectado al cortafuegos de la serie VM, haga clic en **Propiedades**. 3. Resalte el conmutador virtual y haga clic en **Editar**. En las propiedades de vSwitch, haga clic en la ficha **Seguridad**, defina el **Modo promiscuo como Aceptar** y haga clic en **Aceptar**. Este cambio se propagará a todos los grupos de puertos del conmutador virtual. **Para configurar un conmutador virtual distribuido para el modo promiscuo:** 1. Seleccione **Inicio > Inventario > Red**. Resalte el **Grupo de puertos distribuido que desee editar y seleccione la ficha Resumen**. 2. Haga clic en **Editar ajustes** y seleccione **Políticas > Seguridad**, defina el **Modo promiscuo** como **Aceptar** y haga clic en **Aceptar**.

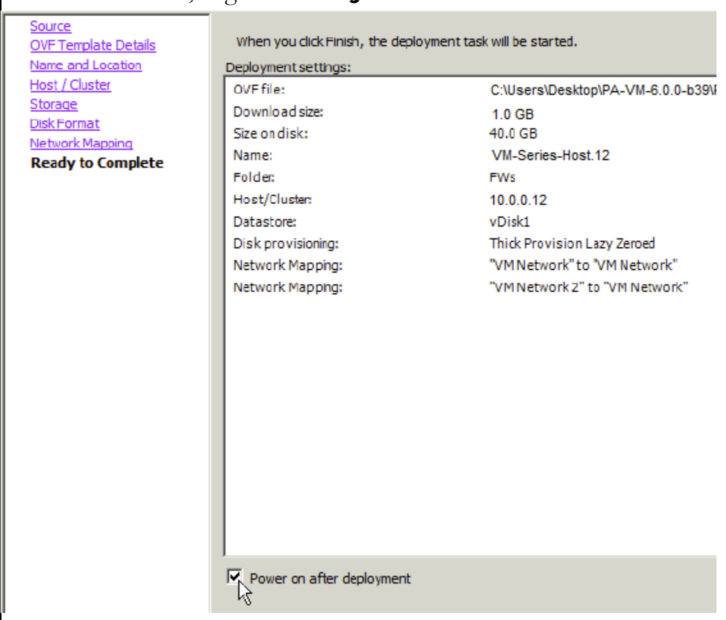
Aprovisionamiento del cortafuegos de la serie VM (Continuación)	
Paso 3 Implemente la plantilla de OVF.	1. Inicie sesión en vCenter mediante el cliente vSphere. También puede ir directamente al host ESXi de destino si es necesario. 2. Desde el cliente vSphere, seleccione **Archivo > Implementar plantilla de OVF**. 3. Desplácese hasta la plantilla de OVF que descargó en el Paso 1, seleccione el archivo y, a continuación, haga clic en **Siguiente**. Revise la ventana de información detallada de las plantillas y, a continuación, vuelva a hacer clic en **Siguiente**. 4. Asigne un nombre a la instancia del cortafuegos de la serie VM y, en la ventana **Ubicación de inventario**, seleccione un centro de datos y carpeta y haga clic en **Siguiente** 5. Seleccione un host ESXi para el cortafuegos de la serie VM y haga clic en **Siguiente**. 6. Seleccione el almacén de datos que se utilizará para el cortafuegos de la serie VM y haga clic en **Siguiente**. 7. Deje la configuración predeterminada para el suministro del almacén de datos y haga clic en **Siguiente**. El valor predeterminado es **Thick Provision Lazy Zeroed**. 

Aprovisionamiento del cortafuegos de la serie VM (Continuación)

8. Seleccione las redes que se utilizarán para las dos vmNIC iniciales. La primera vmNIC se utilizará para la interfaz de gestión y la segunda vmNIC para el primer puerto de datos. Asegúrese de que las **Redes de origen** se asignan a las **Redes de destino** correctas.



9. Revise la ventana de información detallada, haga clic en la casilla de verificación **Activación tras implementación** y, a continuación, haga clic en **Siguiente**.



10. Para ver el progreso de la instalación, supervise la lista **Tareas recientes**. Cuando haya finalizado la implementación, haga clic en la ficha **Resumen** para revisar el estado actual.

Realización de la configuración inicial

Utilice la consola del dispositivo virtual en el servidor ESXi para configurar el acceso de red al cortafuegos de la serie VM. Primero debe configurar la interfaz de gestión y después acceder a la interfaz web para completar más tareas de configuración. Si usa Panorama para la gestión central, consulte la Guía del administrador de Panorama para saber más sobre la gestión del dispositivo mediante Panorama.

Configuración de la interfaz de gestión		
Paso 1	Obtenga la información necesaria de su administrador de red.	• Dirección IP para el puerto MGT • Máscara de red • Puerta de enlace predeterminada • Dirección IP de servidor DNS
Paso 2	Acceda a la consola del cortafuegos de la serie VM.	1. Seleccione la ficha **Consola** en el servidor ESXi para el cortafuegos de la serie VM o haga clic en el botón derecho del cortafuegos de la serie VM y seleccione **Abrir consola**. 2. Pulse Intro para acceder a la pantalla de inicio de sesión. 3. Introduzca el nombre de usuario/contraseña predeterminados (admin/admin) para iniciar sesión. 4. Introduzca **`configurar`** para pasar al modo de configuración.
Paso 3	Defina la configuración de acceso a la red para la interfaz de gestión.	Introduzca el siguiente comando: `set deviceconfig system ip-address <IP-cortafuegos> netmask <máscara de red> default-gateway <IP-puerta de enlace> dns-setting servers primary <IP-DNS>` donde `<IP-cortafuegos>` es la dirección IP que quiere asignar a la interfaz de gestión, `<máscara de red>` es la máscara de subred, `<IP-puerta de enlace>` es la dirección IP de la puerta de enlace de la red y `<IP-DNS>` es la dirección IP del servidor DNS.
Paso 4	Confirme los cambios y salga del modo de configuración.	Introduzca **`commit.`** Introduzca **`exit`**.
Paso 5	Verifique el acceso a la red para los servicios externos requeridos para la gestión del cortafuegos, como el servidor de actualizaciones de Palo Alto Networks.	Para verificar que el cortafuegos tiene acceso de red externa, utilice la utilidad ping utility. Compruebe la conectividad a la puerta de enlace predeterminada, servidor DNS y el servidor de actualización de Palo Alto Networks como se muestra en el siguiente ejemplo: `admin@VM_200-Corp> ping host updates.paloaltonetworks.com` `Haciendo ping a updates.paloaltonetworks.com (67.192.236.252) con 56(84) bytes de datos.` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=40.5 ms` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=53.6 ms` `64 bytes desde 67.192.236.252: icmp_seq=1 ttl=243 tiempo=79.5 ms` **Nota** Cuando haya comprobado la conectividad, pulse Ctrl+C para detener los pings.



Un cortafuegos de la serie VM sin licencia puede procesar hasta 200 sesiones simultáneas. En función del entorno, el límite de sesiones se puede alcanzar muy rápidamente. Por ello, aplique el código de autenticación de capacidad y recupere una licencia antes de comenzar a probar el cortafuegos de la serie VM; de lo contrario puede obtener resultados impredecibles si hay otro tráfico en el grupo de puertos.

Solución de problemas de implementaciones de ESXi

Muchos de los pasos de solución de problemas para el cortafuegos de la serie VM son muy parecidos a los de las versiones de hardware de PAN-OS. Si se produce algún problema, debería comprobar los contadores de la interfaz y archivos de log de sistema y, si es necesario, utilizar la depuración para crear capturas. Si desea más información sobre la solución de problemas de PAN-OS, consulte el artículo de solución de problemas basados en paquetes.

La siguientes secciones describen cómo solucionar algunos problemas comunes:

- Solución de problemas básicos
- Problemas de instalación
- Problemas de licencia
- Problemas de conectividad

Solución de problemas básicos



Recomendación de herramientas de solución de problemas de red
Resulta útil tener una estación de solución de problemas aparte para capturar el tráfico o inyectar paquetes de prueba en el entorno virtualizado. Puede ser útil crear un SO nuevo desde cero con las herramientas de solución de los problemas más comunes instaladas, como tcpdump, nmap, hping, traceroute, iperf, tcpedit, netcat, etc. A continuación esta máquina puede apagarse y convertirse en una plantilla. Cada vez que se necesiten herramientas, el cliente de solución de problemas (máquina virtual) puede implementarse rápidamente en el conmutador virtual en cuestión y usarse para aislar problemas de redes. Cuando la prueba esté completa, la instancia podrá simplemente descartarse y la plantilla se volverá a usar la siguiente vez que sea necesaria.

Para problemas relacionados con el rendimiento en el cortafuegos, primero compruebe el **Panel** en la interfaz web del cortafuegos. Para ver alertas o crear un archivo de asistencia técnica o de volcado de estadísticas, desplácese a **Dispositivo > Asistencia técnica**.

Para obtener información del cliente vSphere, vaya a **Inicio > Inventario > VM y plantillas**, seleccione la instancia del cortafuegos de la serie VM y haga clic en la ficha **Resumen**. Bajo **Recursos**, compruebe las estadísticas de la memoria consumida, la CPU y el almacenamiento. Para conocer el historial de recursos, haga clic en la ficha **Rendimiento** y supervise el consumo de recursos a lo largo del tiempo.

Problemas de instalación

Problemas con la implementación del OVF

La serie VM se proporciona como un archivo descargable de formato abierto de virtualización (OVF). El OVF se descarga como un archivo zip que se extrae en tres carpetas. Si tiene problemas para implementar el OVF, asegúrese de que los tres archivos se extraen y muestran y, si es necesario, vuelva a descargar y extraer el OVF de nuevo.

- La extensión OVF es el archivo descriptivo de OVF que contiene todos los metadatos sobre el paquete y su contenido.
- La extensión MF es el archivo de manifiesto de OVF que contiene los resúmenes de SHA-1 de los archivos individuales del paquete.
- La extensión vmdk es para el archivo de imagen de disco virtual.
- El disco virtual del OVF es mayor para la serie VM; este archivo tiene 900 MB y debe estar presente en el equipo que ejecuta el cliente vSphere. Asegúrese de que la conexión de red es suficiente entre el ordenador cliente de vSphere y el host ESXi de destino. Los cortafuegos de la ruta deben admitir los puertos TCP 902 y 443 del cliente vSphere al host ESXi. Debe haber suficiente ancho de banda y una baja latencia en la conexión, ya que de lo contrario la implementación del OVF puede tardar horas o agotar el tiempo de espera y fallar.

¿Por qué el cortafuegos se inicia en modo de mantenimiento?

Si ha adquirido la licencia del VM-1000-HV y está implementando el cortafuegos de la serie VM en modo independiente en un servidor ESXi de VMware o un servidor SDX de Citrix, debe asignar un mínimo de 5 GB de memoria en el cortafuegos de la serie VM.

Para solucionar este problema, debe modificar el archivo de imagen base (consulte ¿Cómo puedo modificar el archivo de imagen base de la licencia de VM-1000-HV?) o edite los ajustes del host ESXi o el servidor vCenter antes de encender el cortafuegos de la serie VM.

¿Cómo puedo modificar el archivo de imagen base de la licencia de VM-1000-HV?

Si ha adquirido la licencia del VM-1000-HV y está implementando el cortafuegos de la serie VM en modo independiente en un servidor ESXi de VMware o en un servidor SDX de Citrix, siga estas instrucciones para modificar los siguientes atributos que se definen en el archivo de imagen base (.ovf o .xva) del cortafuegos de la serie VM.

Importante: La modificación de valores distintos de los enumerados aquí invalidará el archivo de imagen base.

Modificación del archivo de imagen base (solo si se usa la licencia VM-1000-HV en el modo independiente)	
Paso 1	Abra el archivo de imagen base, por ejemplo 6.0.0, con una herramienta de edición de texto como el bloc de notas.

Modificación del archivo de imagen base (solo si se usa la licencia VM-1000-HV en el modo independiente)
Paso 2 Busque 4096 y cambie la asignación de memoria a 5012 (es decir, 5 GB) aquí:

```
<Item>
 <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
 <rasd:Description>Memory Size</rasd:Description>
 <rasd:ElementName>4096MB of memory</rasd:ElementName>
 <rasd:InstanceID>2</rasd:InstanceID>
 <rasd:ResourceType>4</rasd:ResourceType>
 <rasd:VirtualQuantity>4096</rasd:VirtualQuantity>
<Item>
 <rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
 <rasd:Description>Memory Size</rasd:Description>
 <rasd:ElementName>5102MB of memory</rasd:ElementName>
 <rasd:InstanceID>2</rasd:InstanceID>
 <rasd:ResourceType>5</rasd:ResourceType>
 <rasd:VirtualQuantity>5012</rasd:VirtualQuantity>
```

Paso 3 Cambie el número de núcleos de CPU virtuales que se asignan de 2 a 4 u 8 como desee para su implementación:

```
<Item>
 <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
 <rasd:Description>Number of Virtual CPUs</rasd:Description>
 <rasd:ElementName>2 virtual CPU(s)</rasd:ElementName>
 <rasd:InstanceID>1</rasd:InstanceID>
 <rasd:ResourceType>3</rasd:ResourceType>
 <rasd:VirtualQuantity>2</rasd:VirtualQuantity>
 <vmw:CoresPerSocket ovf:required="false">2</vmw:CoresPerSocket>
 </Item>
<Item>
 <rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
 <rasd:Description>Number of Virtual CPUs</rasd:Description>
 <rasd:ElementName>4 virtual CPU(s)</rasd:ElementName>
 <rasd:InstanceID>1</rasd:InstanceID>
 <rasd:ResourceType>3</rasd:ResourceType>
 <rasd:VirtualQuantity>4</rasd:VirtualQuantity>
 <vmw:CoresPerSocket ovf:required="false">2</vmw:CoresPerSocket>
 </Item>
```

También puede implementar el cortafuegos y antes de activar el cortafuegos de la serie VM, editar la asignación de la CPU virtual y la memoria directamente en el host ESXi o el servidor vCenter.

Problemas de licencia

¿Por qué no puedo aplicar la licencia de funciones o asistencia técnica?

¿Ha aplicado el código de autenticación de capacidad en el cortafuegos de la serie VM? Antes de que pueda activar la licencia de funciones o asistencia técnica, debe aplicar el código de autenticación de capacidad para que el dispositivo pueda obtener un número de serie. Este número de serie es necesario para activar las otras licencias en el cortafuegos de la serie VM.

¿Por qué mi cortafuegos de la serie VM clonado no tiene una licencia válida?

VMware asigna una UUID a cada máquina virtual que incluye el cortafuegos de la serie VM. Así, cuando un cortafuegos de la serie VM se clona, se le asigna una nueva UUID. Como el número de serie y la licencia de cada instancia del cortafuegos de la serie está vinculada a la UUID, si clona el cortafuegos de la serie VM con licencia, el cortafuegos resultante no tendrá una licencia válida. Necesitará un nuevo código de autenticación para activar la licencia en el cortafuegos que acaba de implementar. Debe aplicar el código de autenticación de capacidad y una nueva licencia de asistencia técnica para obtener actualizaciones de funcionalidad, asistencia técnica y software en el cortafuegos de la serie VM.

Problemas de conectividad

¿Por qué el cortafuegos de la serie VM no recibe tráfico de la red?

En el cortafuegos de la serie VM, compruebe los registros de tráfico (**Supervisar > Logs**). Si los logs están vacíos, use el siguiente comando CLI para ver los paquetes de las interfaces del cortafuegos de la serie VM:

show counter global filter delta yes

```
Global counters:
Elapsed time since last sampling: 594,544 seconds

--------------------------------------------------------------------------------
Total counters shown: 0
--------------------------------------------------------------------------------
```

En el entorno vSphere, compruebe lo siguiente:

- Compruebe los grupos de puertos y confirme que el cortafuegos y las máquinas virtuales están en el grupo de puertos correcto.

  Asegúrese de que las interfaces se asignan correctamente.

  Adaptador de red 1 = gestión

  Adaptador de red 2= Ethernet1/1

  Adaptador de red 3= Ethernet1/2

Para cada máquina virtual, compruebe los ajustes para verificar que la interfaz se asigna al grupo de puertos correcto.

- Compruebe que se ha habilitado el modo promiscuo para cada grupo de puertos o para todo el conmutador.

  Como las direcciones MAC de PAN-OS del plano de datos son distintas de las direcciones MAC de VMNIC asignadas por vSphere, el grupo de puertos (o todo el vSwitch) debe estar en modo promiscuo:

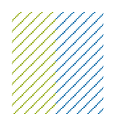
- Compruebe la configuración de VLAN en vSphere.

El uso de la configuración VLAN en el grupo de puertos vSphere tiene dos objetivos: determina qué grupos de puertos comparten un dominio de 2 niveles, y determina si se etiquetan los puertos de vínculo superior (802.1Q).

- Compruebe los ajustes de puerto de conmutador físico.

  Si se especifica una Id. de VLAN en un grupo de puertos con puertos de vínculo superior, vSphere usará 802.1Q para etiquetar las tramas salientes. La etiqueta debe coincidir con la configuración del conmutador físico, de lo contrario el tráfico no pasará.

  Compruebe las estadísticas del puerto si usa conmutadores distribuidos virtuales (vDS); los conmutadores estándar no proporcionan estadísticas de puerto.



Configuración de un Cortafuegos de la serie VM en el servidor Citrix SDX

Para reducir el impacto ecológico y consolidar funciones clave en un único servidor, puede implementar una o varias instancias del cortafuegos de la serie VM en el servidor Citrix SDX. La implementación del cortafuegos de la serie VM junto con la NetScaler VPX garantiza el suministro de aplicaciones, además de la seguridad de red, disponibilidad, rendimiento y visibilidad.

- ▲ Acerca del cortafuegos de la serie VM en el servidor SDX
- ▲ Requisitos y limitaciones del sistema
- ▲ Implementaciones compatibles
- ▲ Instalación del Cortafuegos de la serie VM
- ▲ Tráfico norte-sur seguro con el cortafuegos de la serie VM
- ▲ Tráfico este-oeste con el cortafuegos de la serie VM

Acerca del cortafuegos de la serie VM en el servidor SDX

Se pueden implementar una o varias instancias del cortafuegos de la serie VM para garantizar el tráfico este-oeste o norte-sur en la red; son compatibles las interfaces de cable virtual, interfaces de la capa 2 y de la capa 3. Para implementar el cortafuegos, consulte Instalación del Cortafuegos de la serie VM.

Una vez implementado, el cortafuegos de la serie VM funciona de forma sincronizada con la NetScaler VPX (si es necesario), un dispositivo virtual de NetScaler implementado en el servidor SDX. La NetScaler VPX proporciona equilibro de carga y una función de gestión de tráfico y suele implementarse frente a una granja de servidores para facilitar un acceso eficaz a los servidores. Para obtener una visión general completa de las funciones de NetScaler, consulte http:www.citrix.com/netscaler. Cuando la serie VM se utiliza conjuntamente para trabajar con la NetScaler VPX, las funciones complementarias mejoran su gestión del tráfico, el equilibro de la carga y las necesidades de seguridad de la aplicación/red.

Este documento asume su familiaridad con la red y la configuración en la NetScaler VPX. Con el fin de proporcionar contexto para los términos utilizados en esta sección, a continuación presentamos una breve actualización sobre las direcciones de IP propiedad de NetScaler a las que se se hace referencia en este documento:

- Direcciones IP de NetScaler (NSIP): NSIP es la dirección IP para el acceso de gestión y sistema general al propio NetScaler y para la comunicación de alta disponibilidad.
- Dirección IP asignada (MIP): Una MIP se utiliza para las conexiones en la parte del servidor. No es la dirección IP de NetScaler. En la mayoría de los casos, cuando NetScaler recibe un paquete, sustituye la dirección IP de origen por una MIP antes de enviar el paquete al servidor. Con los servidores abstraídos de los clientes, NetScaler gestiona las conexiones con mayor eficacia.
- Dirección IP del servidor virtual (VIP): Una VIP es la dirección IP asociada con un servidor. Es la dirección IP pública a la que se conectan los clientes. Puede que una instancia de NetScaler que gestiona una amplia variedad de tráfico tenga muchas VIP configuradas.
- Dirección IP de subred (SNIP): Cuando NetScaler se adjunta a varias subredes, las SNIP se pueden configurar para utilizarse como MIP que proporcionan acceso a estas subredes. Las SNIP pueden estar vinculadas a VLAN e interfaces específicas.

Para obtener ejemplos sobre cómo implementar de forma conjunta el cortafuegos de la serie VM y la NetScaler VPX, consulte Implementaciones compatibles.

Requisitos y limitaciones del sistema

Esta sección enumera los requisitos y las limitaciones del cortafuegos de la serie VM en el servidor Citrix SDX.

Requisitos

Puede implementar varias instancias del cortafuegos de la serie VM en el servidor Citrix SDX. Como todas las instancias del cortafuegos necesitan una asignación de recursos mínima (cantidad de CPU, memoria y espacio en disco) en el servidor SDX, asegúrese de cumplir las especificaciones que aparecen a continuación para garantizar un rendimiento óptimo.

Requisito	Detalle
Plataformas SDX	• 11500, 13500, 14500, 16500, 18500, 20500; • 17550, 19550, 20550, 21550
Versión de SDX	10.1+ 10.1 no es compatible; se necesita una versión de software superior a 10.1.
Versión de Citrix XenServer	6.0.2 o superior
Recursos mínimos del sistema **Nota** Planee y asigne el número total de interfaces de datos que podría necesitar en el cortafuegos de la serie VM. Esta tarea es básica durante la implementación inicial, porque añadir o eliminar interfaces del cortafuegos de la serie VM después de la implementación inicial hará que las interfaces de datos (Eth 1/1 y Eth 1/2) del cortafuegos de la serie VM reasigne a los adaptadores en el servidor SDX. Todas las interfaces de datos se asignan secuencialmente al adaptador con el valor numérico más bajo. Esta reasignación puede producir un fallo de coincidencia en la configuración del cortafuegos.	• Dos vCPU por cortafuegos de la serie VM. Una se utilizará para el plano de gestión y la otra para el plano de datos. Puede añadir cualquier vCPU en las siguientes combinaciones: 2, 4 u 8 vCPU; se asignan vCPU adicionales al plano de datos. • Dos interfaces de red: una dedicada al tráfico de gestión y otra para el tráfico de datos. Con el tráfico de gestión puede utilizar las interfaces 0/x en el plano de gestión o las interfaces 10/x en el plano de datos. Asigne interfaces de red adicionales para el tráfico de datos, según lo necesite su topología de red. • 4 GB de memoria. Cualquier memoria adicional que asigne se utilizará únicamente en el plano de gestión. • Un mínimo de 40 GB de espacio de disco virtual. Puede añadir hasta 2 TB de espacio en disco; cualquier espacio por encima del requisito mínimo de 40 GB solo se utilizará para creación de logs.

Limitaciones

El cortafuegos de la serie VM implementado en el servidor Citrix SDX tiene las siguientes limitaciones:

- Se puede configurar un máximo de 24 puertos. Se utilizará uno para el tráfico de gestión y hasta 23 para el tráfico de datos.
- No se admiten tramas gigantes.
- No se admite la agregación de enlaces.

Implementaciones compatibles

En las siguientes situaciones, el cortafuegos de la serie VM asegura el tráfico destinado a los servidores de la red. Funciona junto con la NetScaler VPX para gestionar el tráfico antes o después de que alcance a la NetScaler VPX.

- Situación 1: Tráfico norte-sur seguro
- Situación 2: Tráfico este-oeste seguro

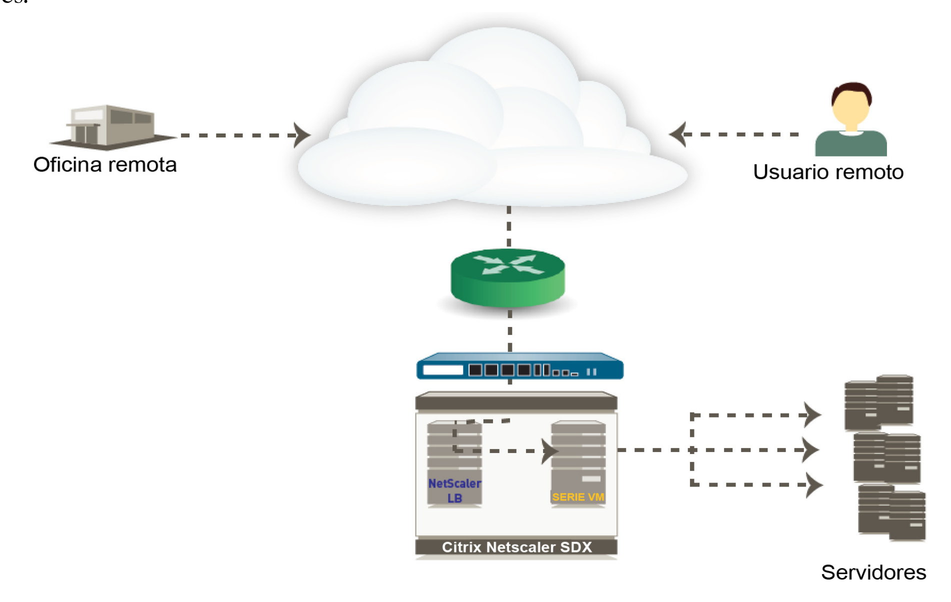
Situación 1: Tráfico norte-sur seguro

Para garantizar el tráfico norte-sur, tiene las siguientes opciones:

- Cortafuegos de la serie VM entre la NetScaler VPX y los servidores
- Cortafuegos de la serie VM antes de la NetScaler VPX

Cortafuegos de la serie VM entre la NetScaler VPX y los servidores

El cortafuegos del perímetro acota todo el tráfico en la red. Todo el tráfico permitido en la red fluye a través de la NetScaler VPX y, a continuación, a través del cortafuegos de la serie VM antes de que la solicitud se envíe a los servidores.



En esta situación, el cortafuegos de la serie VM asegura el tráfico norte-sur y se puede implementar usando las interfaces de cable virtual, de la capa 2 y la capa 3.

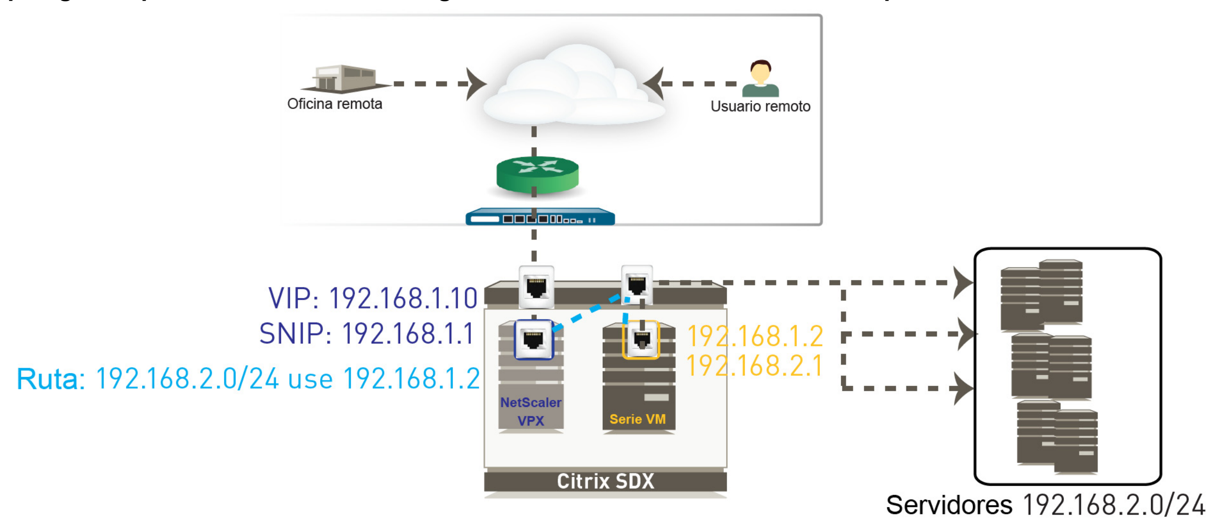
- Cortafuegos de la serie VM con interfaces de capa 3
- Cortafuegos de la serie VM con interfaces de capa 2 o cable virtual

Cortafuegos de la serie VM con interfaces de capa 3

La implementación del cortafuegos con interfaces de capa 3 le permite ampliar capacidad más fácilmente, conforme implemente nuevos servidores y subredes. Puede implementar varias instancias del cortafuegos para gestionar el tráfico a cada nueva subred y, a continuación, configurar los cortafuegos como par de alta disponibilidad, si es necesario.

El uso de una interfaz de L3 le permite realizar cambios mínimos en la configuración de servidor/red de SDC porque la SNIP, para alcanzar los servidores, se elimina de la NetScaler VPX y se configura en el cortafuegos de la serie VM. Con este método, solo se utiliza una interfaz de datos en el cortafuegos de la serie VM, por lo que solo se puede definir una zona. Como resultado, cuando se definen las reglas de la política, debe especificar la dirección IP/subredes de origen y destino en las que aplicar las reglas de seguridad. Para obtener más información, consulte Implementación del cortafuegos de la serie VM con interfaces de capa 3.

Topología después de añadir el cortafuegos de la serie VM con interfaces de capa 3



En este ejemplo, la dirección IP pública a la que se conecta el cliente (VIP en la NetScaler VPX) es 192.168.1.10. Para proporcionar acceso a los servidores de la subred 192.168.2.x, la configuración de la VPX hace referencia a las subredes (SNIP) 192.168.1.1 y 192.168.2.1. Según su configuración de red y rutas predeterminadas, es posible que deba modificar la ruta de los servidores.

Cuando configura el cortafuegos de la serie VM, debe añadir una interfaz de datos (por ejemplo, eth1/1) y asignar dos direcciones IP a la interfaz. Una dirección IP debe estar en la misma subred que la VIP y la otra debe estar en la misma subred que los servidores. En este ejemplo, las direcciones IP asignadas a las interfaces de datos son 192.168.1.2 y 192.168.2.1. Como solo se utiliza una interfaz de datos en el cortafuegos de la serie VM, todo el tráfico pertenece a una única zona y todo el tráfico interno de la zona se permite implícitamente en la política. Por lo tanto, cuando se definen las reglas de la política, debe especificar la dirección IP/subredes de origen y destino en las que aplicar las reglas de seguridad.

Incluso después de que haya añadido el cortafuegos de la serie VM al servidor SDX, la dirección IP a la que continúan conectándose los clientes es la VIP de la NetScaler VPX (192.168.1.10). Sin embargo, para dirigir todo el tráfico a través del cortafuegos, debe definir una ruta a la subred 192.168.2.x en la NetScaler VPX. En este ejemplo, para acceder a los servidores, esta ruta debe hacer referencia a la dirección IP 192.168.1.2 asignada a la interfaz de datos del cortafuegos de la serie VM. Ahora, todo el tráfico destinado a los servidores se dirige desde la NetScaler VPX al cortafuegos y, a continuación, a los servidores. El tráfico de retorno utiliza la interfaz 192.168.2.1 en la serie VM y utiliza la SNIP 192.168.1.1 como su siguiente salto.



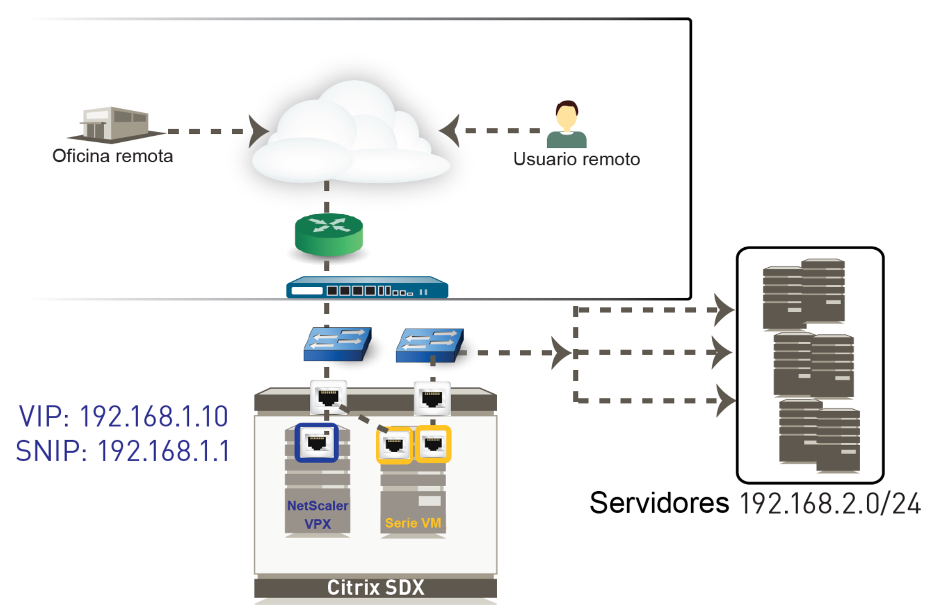
Para cumplir con los requisitos de seguridad, si la opción USIP (Usar IP de origen de cliente) está habilitada en la NetScaler VPX, entonces el cortafuegos de la serie VM necesita una ruta predeterminada que apunte a la SNIP 192.168.1.1, en este ejemplo. Si se utiliza una dirección IP de NAT predeterminada (asignada/SNIP), no tendrá que definir una ruta predeterminada en el cortafuegos de la serie VM.

Para obtener instrucciones, consulte Implementación del cortafuegos de la serie VM con interfaces de capa 3.

Cortafuegos de la serie VM con interfaces de capa 2 o cable virtual

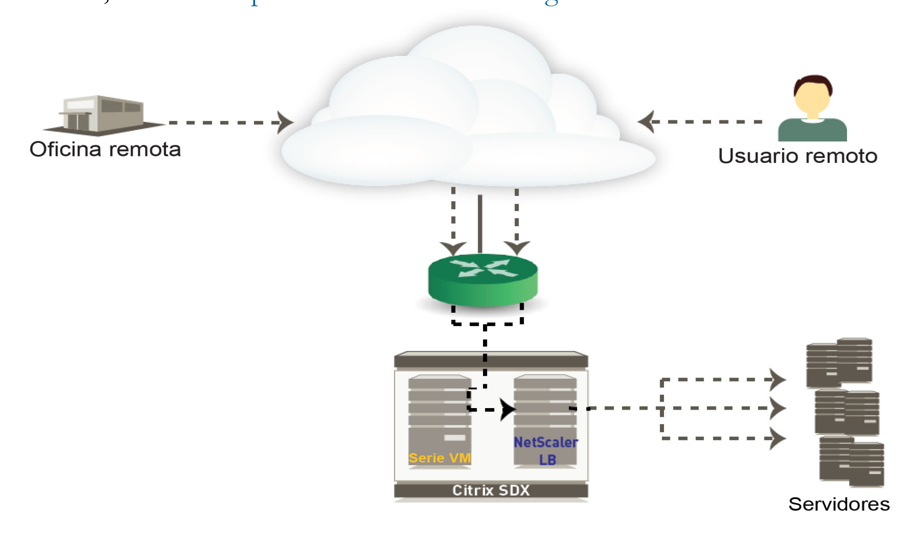
La implementación del cortafuegos de la serie VM con interfaces de capa 2 o de cable virtual necesita que reconfigure la NetScaler VPX para eliminar la conexión directa a los servidores. En ese momento, el cortafuegos de la serie VM ya se puede cablear y configurar para interceptar de forma transparente y aplicar la política al tráfico destinado a los servidores. En este método, se crean dos interfaces de datos en el cortafuegos, cada una perteneciente a una zona distinta. La política de seguridad se define para permitir el tráfico entre las zonas de origen y destino. Para obtener más información, consulte Implementación del cortafuegos de la serie VM con interfaces de capa 2 (L2) o de cable virtual.

Topología después de añadir el cortafuegos de la serie VM con interfaces de capa 2 o cable virtual



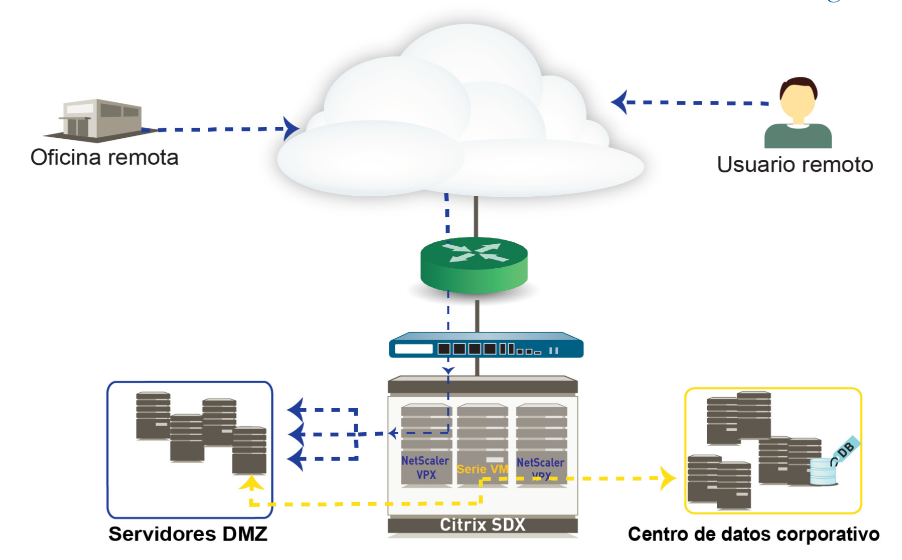
Cortafuegos de la serie VM antes de la NetScaler VPX

En esta situación, al cortafuegos del perímetro lo sustituye el cortafuegos de la serie VM, que se puede implementar usando las interfaces de cable virtual, de capa 3 o de capa 2. El cortafuegos de la serie VM asegura todo el tráfico de la red antes de que la solicitud alcance la NetScaler VPX y se envíe a los servidores. Para obtener más información, consulte Implementación del cortafuegos de la serie VM antes de la NetScaler VPX.



Situación 2: Tráfico este-oeste seguro

El cortafuegos de la serie VM se implementa junto con dos sistemas de la NetScaler VPX que prestan servicio a distintos segmentos del servidor de su red o que funcionan como puntos de terminación para los túneles SSL. En esta situación, el cortafuegos del perímetro garantiza el tráfico entrante. Entonces, el tráfico destinado a los servidores de DMZ fluye a una NetScaler VPX que equilibra las cargas de la solicitud. Para añadir una capa adicional de seguridad a la red interna, todo el tráfico este-oeste entre DMZ y la red corporativa se enruta a través del cortafuegos de la serie VM. El cortafuegos puede aplicar la seguridad de red y validar el acceso para ese tráfico. Para obtener más información, consulte Tráfico este-oeste con el cortafuegos de la serie VM.



Instalación del Cortafuegos de la serie VM

Se necesita una cuenta de asistencia y una licencia de la serie VM válida para obtener el archivo .xva de imagen base necesario para instalar el cortafuegos de la serie VM en el servidor SDX. Si no ha registrado todavía el código de autenticación de capacidad que ha recibido con el correo electrónico de cumplimiento del pedido, con su cuenta de asistencia, consulte Registro del cortafuegos de la serie VM. Después de completar el registro, continúe realizando las siguientes tareas:

- Carga de la imagen en el servidor SDX
- Aprovisionamiento del cortafuegos de la serie VM

Carga de la imagen en el servidor SDX

Para aprovisionar el cortafuegos de la serie VM, debe obtener el archivo de imagen .xva y cargarlo al servidor SDX.

Carga de la imagen XVA en el servidor SDX		
Paso 1	Descargue y extraiga el archivo .zip de imagen base en un ordenador local.	1. Vaya a https://support.paloaltonetworks.com/ y descargue el archivo .zip de **imagen base de Citrix SDX de la serie VM**. 2. Descomprima el archivo zip de la imagen base y extraiga el archivo **.xva**. Este archivo .xva es necesario para instalar el cortafuegos de la serie VM.
Paso 2	Cargue la imagen del ordenador local al servidor Citrix SDX.	1. Inicie el navegador web e inicie sesión en el servidor SDX. 2. Seleccione **Configuración > Serie VM de Palo Alto > Imágenes de software**. 3. En el menú desplegable **Acción**, seleccione **Cargar**... y **navegue** hasta la ubicación del archivo de imagen *.xva* guardado. 4. Seleccione la imagen y haga clic en **Abrir**. 5. **Cargue** la imagen en el servidor SDX.

Aprovisionamiento del cortafuegos de la serie VM

Aprovisionamiento del cortafuegos de la serie VM en el servidor SDX	
Paso 1 Acceda al servidor SDX.	Inicie el navegador web y conecte al servidor SDX.
Paso 2 Cree el cortafuegos de la serie VM. **Nota** Asigne el número total de interfaces de datos que podría necesitar en el cortafuegos de la serie VM durante la implementación inicial. Añadir o eliminar interfaces al cortafuegos de la serie VM después de la implementación inicial hará que las interfaces de datos (Eth 1/1 y Eth 1/2) del cortafuegos de la serie VM reasigne a los adaptadores en el servidor SDX. Cada interfaz de datos asigna secuencialmente al adaptador el valor numérico más bajo y puede, por tanto, producir un fallo de coincidencia en la configuración del cortafuegos.	1. Seleccione **Configuración > Serie VM de Palo Alto > Instancias** 2. Haga clic en **Añadir.** 3. Introduzca un nombre para el cortafuegos de la serie VM. 4. Seleccione la imagen .xva que había cargado anteriormente. Esta imagen es necesaria para abastecer el cortafuegos. 5. Asigne memoria, espacio en disco adicional y CPU virtuales para el cortafuegos de la serie VM. Para verificar las recomendaciones de asignación de recursos, consulte Requisitos. 6. Seleccione las interfaces de red. a. Utilice las interfaces de gestión 0/1 o 0/2 y asigne una dirección IP, una máscara de red y una dirección IP de puerta de enlace. **Nota** Si es necesario, puede utilizar una interfaz de datos en el servidor SDX para gestionar el cortafuegos. b. Seleccione las interfaces de datos que se utilizarán para gestionar el tráfico hacia y desde el cortafuegos. **Nota** Si planea implementar las interfaces como capa 2 o de cable virtual, seleccione la opción **Permitir modo de capa 2** de forma que el cortafuegos pueda recibir y reenviar los paquetes para direcciones MAC que no sean las propias. 7. Revise el resumen y haga clic en **Finalizar** para comenzar el proceso de instalación. Lleva 5-8 minutos aprovisionar el cortafuegos. Cuando termine, utilice la dirección IP de gestión para iniciar la interfaz web del cortafuegos.

Continúe con la Activación de la licencia.

Tráfico norte-sur seguro con el cortafuegos de la serie VM

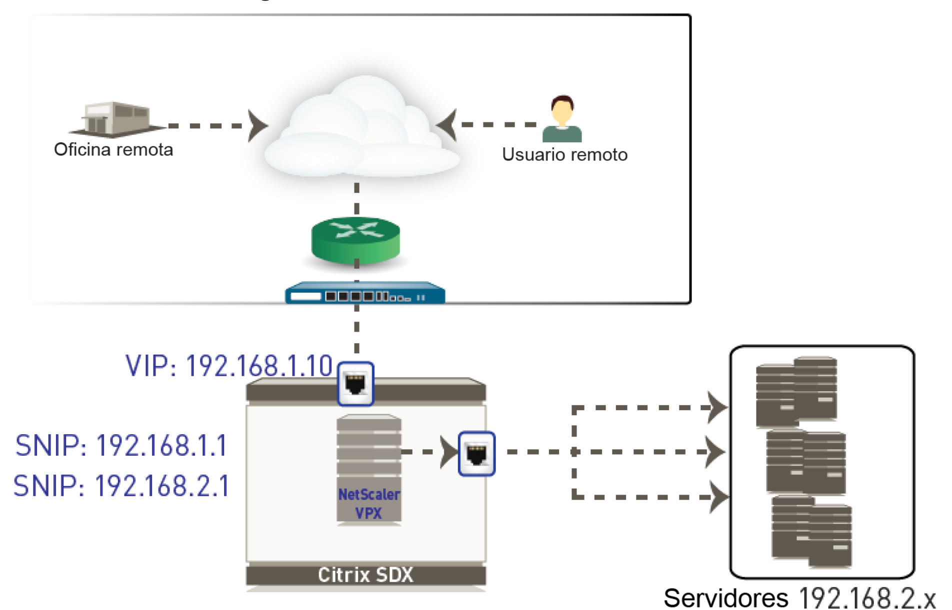
Esta sección incluye información sobre las siguientes implementaciones:

- Implementación del cortafuegos de la serie VM con interfaces de capa 3
- Implementación del cortafuegos de la serie VM con interfaces de capa 2 (L2) o de cable virtual
- Implementación del cortafuegos de la serie VM antes de la NetScaler VPX (con interfaces de cable virtual)

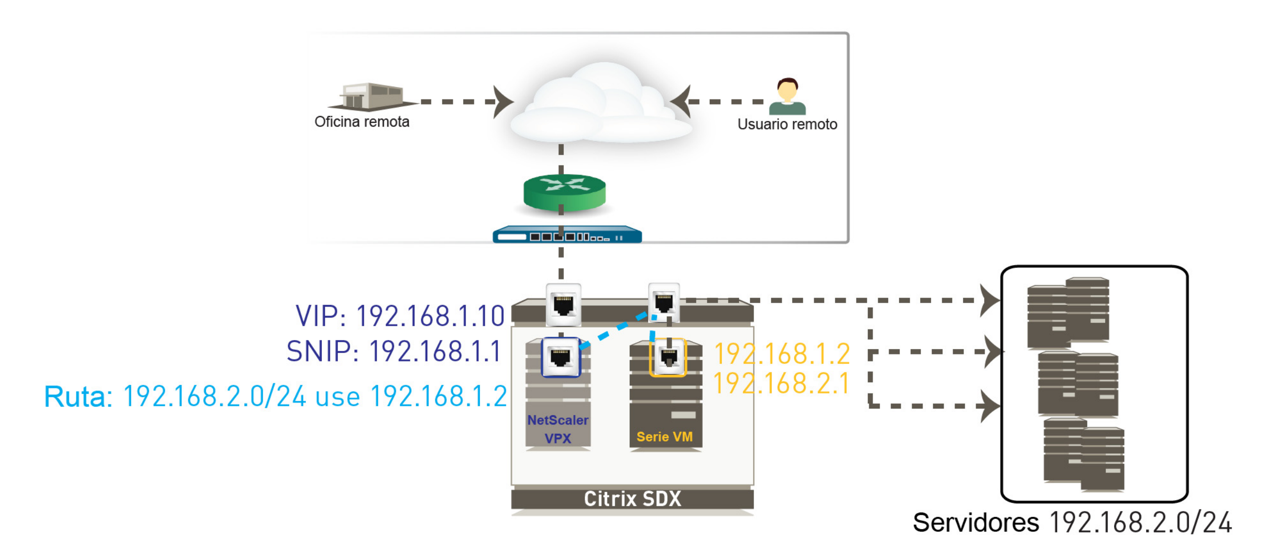
Implementación del cortafuegos de la serie VM con interfaces de capa 3

Para asegurar el tráfico norte-sur, esta situación le muestra cómo implementar el cortafuegos de la serie VM con capa 3; el cortafuegos de la serie VM se coloca para asegurar el tráfico entre la NetScaler VPX y los servidores de la red.

Topología antes de añadir el cortafuegos de la serie VM



Topología después de añadir el cortafuegos de la serie VM



En la siguiente tabla se incluyen las tareas que debe realizar para implementar el cortafuegos de la serie VM. Para obtener instrucciones de configuración del cortafuegos, consulte la Guía de inicio de PAN-OS. El flujo de trabajo y la configuración de la NetScaler VPX no se explican en este documento; para obtener más información sobre cómo configurar la NetScaler VPX, consulte la documentación de Citrix.

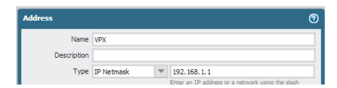
Configuración del cortafuegos de la serie VM para procesar tráfico norte-sur usando las interfaces de la capa 3		
Paso 1	Instalación del Cortafuegos de la serie VM.	Cuando aprovisiona el cortafuegos de la serie VM en el servidor SDX, debe asegurarse de seleccionar la interfaz de datos con precisión para que el cortafuegos pueda acceder a los servidores.
Paso 2	Configure la interfaz de datos en el cortafuegos.	1. Seleccione **Red > Enrutador virtual** y, a continuación, seleccione el enlace **predeterminado** para abrir el cuadro de diálogo Enrutador virtual y **añada** la interfaz al enrutador virtual. 2. (Solo es necesario si la opción USIP está habilitada en la NetScaler VPX) En la ficha **Rutas estáticas** del enrutador virtual, seleccione la interfaz y añada la NetScaler SNIP (192.68.1.1 en este ejemplo) como **Siguiente salto**. La ruta estática definida aquí se utilizará para dirigir el tráfico desde el cortafuegos hasta la NetScaler VPX. 3. Seleccione **Red > Interfaces > Ethernet** y, a continuación, seleccione la interfaz que quiera configurar. 4. Seleccione el **Tipo de interfaz**. Aunque su decisión aquí depende de la topología de su red, este ejemplo utiliza **Capa3**. 5. En la ficha **Configuración**, en el menú desplegable **Enrutador virtual**, seleccione **predeterminado**. 6. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**. En el cuadro de diálogo Zona, defina un **Nombre** para una nueva zona, por ejemplo "Predeterminado" y, a continuación, haga clic en **Aceptar**. 7. Seleccione la ficha **IPv4 o IPv6**, haga clic en **Añadir** en la sección IP e introduzca las dos direcciones IP y la máscara de red para la interfaz (una para cada subred a la que se esté dando servicio). Por ejemplo, 192.168.1.2 y 192.168.2.1.
		8. (Optativo) Para permitirle hacer ping o usar SSH en la interfaz, seleccione **Avanzada > Otra información**, abra el menú desplegable **Perfil de gestión** y seleccione el **Nuevo perfil de gestión**. Introduzca un **nombre** para el perfil, seleccione **Ping** y **SSH** y, a continuación, haga clic en **Aceptar**. 9. Para guardar la configuración de la interfaz, haga clic en **Aceptar**. 10. Haga clic en **Compilar** para guardar sus cambios en el cortafuegos.

Configuración del cortafuegos de la serie VM para procesar tráfico norte-sur usando las interfaces de la capa 3

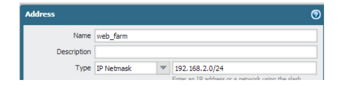
Paso 3 Cree una política básica que permita el tráfico entre la NetScaler VPX y los servidores web.

En este ejemplo, debido a que solo hemos configurado una interfaz de datos, especificamos la dirección IP de destino y de origen para permitir el tráfico entre la NetScaler VPX y los servidores.

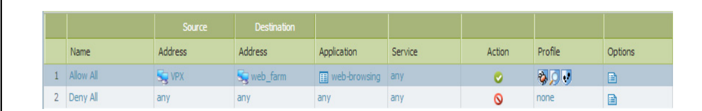
1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir**.
2. Asigne a la regla un nombre descriptivo en la pestaña **General**.
3. En la ficha **Origen**, seleccione **Añadir** en la sección Dirección de origen y seleccione el enlace de nueva **dirección**.
4. Cree un objeto de nueva dirección que especifique la SNIP en la NetScaler VPX. En este ejemplo, esta dirección IP es el origen de todas las solicitudes para los servidores.



5. En la ficha **Destino**, seleccione **Añadir** en la sección Dirección de destino y seleccione el enlace de nueva **dirección**.
6. Cree un objeto de nueva dirección que especifique la subred de los servidores web. En este ejemplo, esta subred alberga todos los servidores web que atienden las solicitudes.



7. En la ficha **Aplicación**, seleccione la navegación web.
8. En la pestaña **Acciones**, realice estas tareas:
   a. Establezca **Configuración de acción** como **Permitir**.
   b. Adjunte los perfiles predeterminados para la protección antivirus y contra vulnerabilidades dentro de **Ajuste de perfil**.
9. Verifique que los logs están habilitados al final de una sesión bajo **Opciones**. Únicamente se registrará el tráfico que coincida con una regla de seguridad.



		Source	Destination					
	Name	Address	Address	Application	Service	Action	Profile	Options
1	Allow All	VPX	web_farm	web-browsing	any			
2	Deny All	any	any	any	any		none	

10. Cree otra regla para denegar cualquier otro tráfico de cualquier dirección IP de origen y de destino de la red.

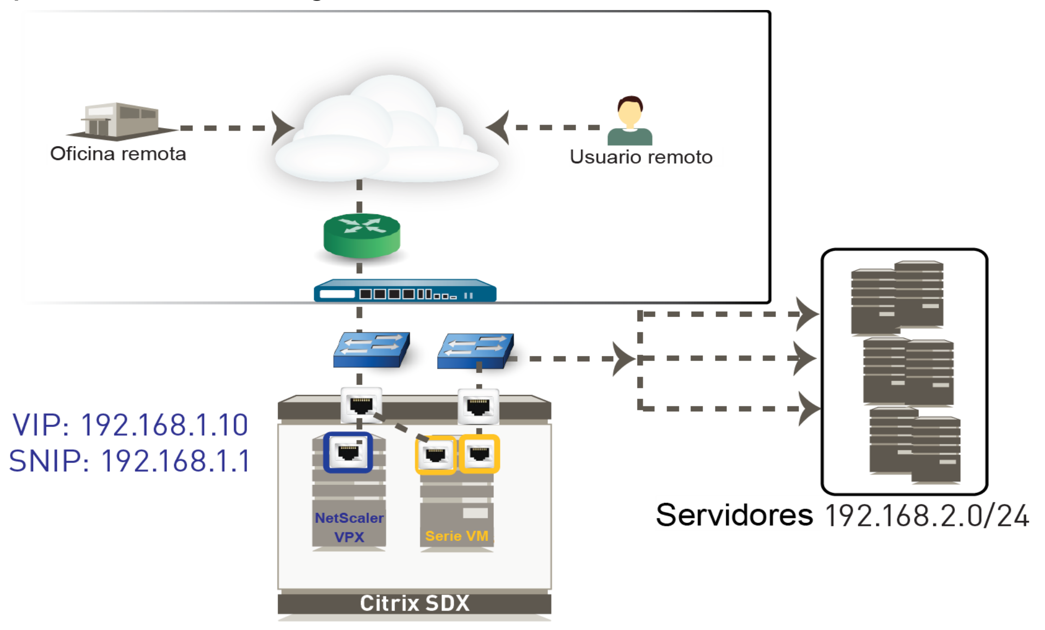
    Como todo el tráfico interno de la zona está permitido de forma predeterminada, para poder denegar tráfico no relacionado con la navegación web, debe crear una regla de denegación que bloquee explícitamente el resto del tráfico.

Implementación del cortafuegos de la serie VM con interfaces de capa 2 (L2) o de cable virtual

Para asegurar el tráfico norte-sur, esta situación le muestra cómo implementar el cortafuegos de la serie VM en una implementación de capa 2 o de cable virtual. El cortafuegos de la serie VM asegura el tráfico destinado a los servidores. La solicitud llega a la dirección VIP de la NetScaler VPX y la procesa el cortafuegos de la serie VM antes de que alcance los servidores. En la ruta de retorno, el tráfico se dirige a la SNIP en la NetScaler VPX y el cortafuegos de la serie VM lo procesa antes de que el cliente lo reciba de vuelta.

Para conocer la topología antes de añadir el cortafuegos de la serie VM, consulte Topología antes de añadir el cortafuegos de la serie VM.

Topología después de añadir el cortafuegos de la serie VM



En la siguiente tabla se incluyen las tareas básicas de configuración que debe realizar para implementar el cortafuegos de la serie VM. Para obtener instrucciones de configuración del cortafuegos, consulte la Guía de inicio de PAN-OS. El flujo de trabajo y la configuración de la NetScaler VPX no se explican en este documento; para obtener más información sobre cómo configurar la NetScaler VPX, consulte la documentación de Citrix.

Configuración del cortafuegos de la serie VM para procesar tráfico norte-sur usando la interfaces de la capa 2 o cable virtual		
Paso 1	Instalación del Cortafuegos de la serie VM.	En el servidor SDX, asegúrese de habilitar **Permitir modo de capa 2** en todas las interfaces de datos. Este ajuste permite al cortafuegos sortear paquetes destinados a la VIP de NetScaler VPX.

Configuración del cortafuegos de la serie VM para procesar tráfico norte-sur usando la interfaces de la capa 2 o cable virtual (Continuación)

Paso 2 Vuelva a conectar el cable a la interfaz de la parte del servidor asignada a la NetScaler VPX.

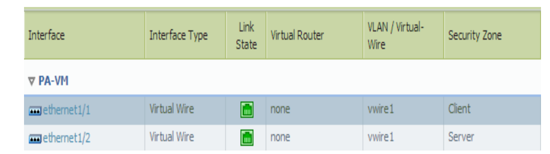
Como la NetScaler VPX se reiniciará cuando vuelva a conectarse el cable, evalúe si desea realizar esta tarea durante una ventana de mantenimiento.

Si ya ha implementado una NetScaler VPX y ahora está añadiendo el cortafuegos de la serie VM al servidor SDX, tendrá dos puertos asignados a la VPX. Cuando implemente el cortafuegos de la serie VM, la NetScaler VPX solo necesitará un puerto para gestionar el tráfico de la parte del cliente.

Por lo tanto, antes de configurar las interfaces de datos de la serie VM, debe retirar el cable de la interfaz que conecta la VPX a la granja de servidores y conectarlo al cortafuegos para que este procese todo el tráfico dirigido a la granja de servidores.

Paso 3 Configure las interfaces de datos.

En este ejemplo se muestra la configuración para las interfaces de cable virtual.



Interface	Interface Type	Link State	Virtual Router	VLAN / Virtual-Wire	Security Zone
▽ PA-VM					
ethernet1/1	Virtual Wire		none	vwire1	Client
ethernet1/2	Virtual Wire		none	vwire1	Server

1. Inicie la interfaz web del cortafuegos.
2. Seleccione **Red > Interfaces > Ethernet**.
3. Haga clic en el enlace de una interfaz (por ejemplo, ethernet 1/1) y seleccione el **tipo de interfaz** como de **capa 2** o **cable virtual**.

Configuración de cable virtual

Todas las interfaces de cable virtual (ethernet 1/1 y ethernet 1/2) deben conectarse a una zona de seguridad y un cable virtual. Para configurar estos ajustes, seleccione la ficha **Configuración** y complete las siguientes tareas:

a. En el menú desplegable Cable virtual haga clic en **Nuevo cable virtual**, defina un **nombre**, asígnele las dos interfaces de datos (ethernet 1/1 y ethernet 1/2) y, a continuación, haga clic en **Aceptar**.
Cuando configure ethernet 1/2, seleccione este cable virtual.

b. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **nombre** para la nueva zona, por ejemplo *cliente* y, a continuación, haga clic en **Aceptar**.

Configuración de capa 2

Necesita una zona de seguridad en cada interfaz de capa 2. Seleccione la ficha **Configuración** y complete las siguientes tareas:

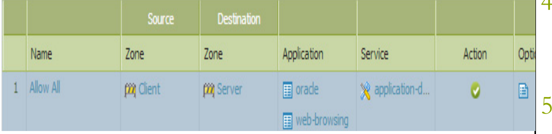
a. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **nombre** para la nueva zona, por ejemplo *cliente* y, a continuación, haga clic en **Aceptar**.

4. Repita los pasos 2 y 3 que aparecen anteriormente para la otra interfaz.
5. Haga clic en **Compilar** para guardar los cambios en el cortafuegos.

Configuración del cortafuegos de la serie VM para procesar tráfico norte-sur usando la interfaces de la capa 2 o cable virtual (Continuación)

Paso 4 Cree una regla de política básica que permita el tráfico a través del cortafuegos.

En este ejemplo se muestra cómo permitir el tráfico entre la NetScaler VPX y los servidores web.

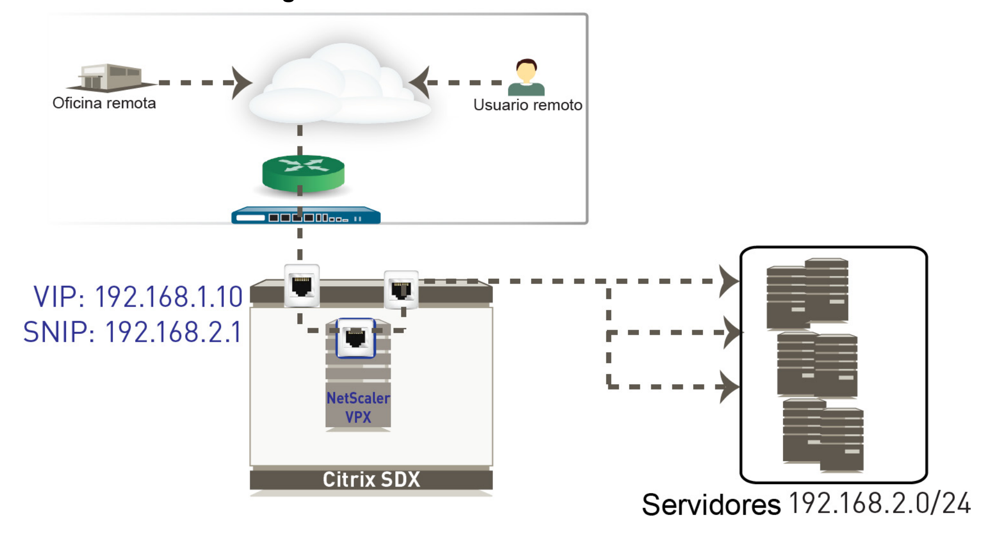


1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir**.
2. Asigne a la regla un nombre descriptivo en la pestaña **General**.
3. En la ficha **Origen**, establezca la **zona de origen** para la zona de la parte del cliente que ha definido. En este ejemplo, seleccione el cliente.
4. En la ficha **Destino**, establezca la **zona de destino** para la zona de la parte del servidor que ha definido. En este ejemplo, seleccione el servidor.
5. En la ficha **Aplicación**, haga clic en **Añadir** para seleccionar las aplicaciones a las que debe permitir el acceso.
6. En la pestaña **Acciones**, realice estas tareas:
   a. Establezca **Configuración de acción** como **Permitir**.
   b. Adjunte los perfiles predeterminados para la protección antivirus, antispyware y contra vulnerabilidades y para el filtrado de URL, en **Ajuste de perfil**.
7. Verifique que los logs están habilitados al final de una sesión bajo **Opciones**. Únicamente se registrará el tráfico que coincida con una regla de seguridad.

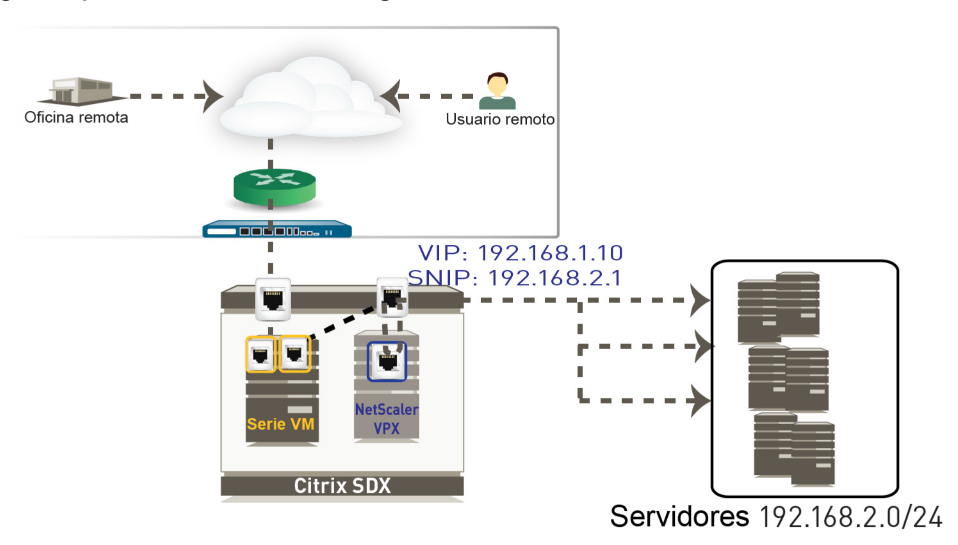
Implementación del cortafuegos de la serie VM antes de la NetScaler VPX

En el siguiente ejemplo se muestra cómo implementar el cortafuegos de la serie VM para procesar y asegurar el tráfico antes de que alcance la NetScaler VPX. En este ejemplo, el cortafuegos de la serie VM se implementa con las interfaces de cable virtual y las solicitudes de conexión del cliente se destinan a la VIP de la NetScaler VPX. Observe que puede implementar el cortafuegos de la serie VM usando las interfaces de capa 2 o capa 3, basadas en necesidades específicas.

Topología antes de añadir el cortafuegos de la serie VM



Topología después de añadir el cortafuegos de la serie VM



En la siguiente tabla se incluyen las tareas básicas de configuración que debe realizar en el cortafuegos de la serie VM. Para obtener instrucciones de configuración del cortafuegos, consulte la Guía de inicio de PAN-OS. El flujo de trabajo y la configuración de la NetScaler VPX no se explican en este documento; para obtener más información sobre cómo configurar la NetScaler VPX, consulte la documentación de Citrix.

Configuración del cortafuegos de la serie VM antes de la NetScaler VPX con interfaces de cable virtual		
Paso 1	Instalación del Cortafuegos de la serie VM.	En el servidor SDX, asegúrese de habilitar **Permitir modo de capa 2** en la interfaz de datos. Este ajuste permite al cortafuegos sortear paquetes destinados a la VIP de NetScaler VPX.

Configuración del cortafuegos de la serie VM antes de la NetScaler VPX con interfaces de cable virtual

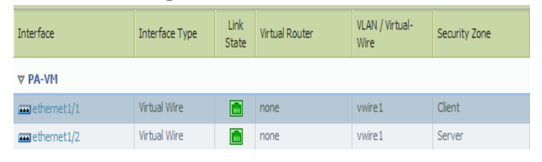
Paso 2 Vuelva a conectar el cable a la interfaz de la parte del cliente asignada a la NetScaler VPX.

Como la NetScaler VPX se reiniciará cuando vuelva a conectarse el cable, evalúe si desea realizar esta tarea durante una ventana de mantenimiento.

Si ya ha implementado una NetScaler VPX y ahora está añadiendo el cortafuegos de la serie VM al servidor SDX, tendrá dos puertos asignados a la VPX. Cuando implementa el cortafuegos de la serie VM, la NetScaler VPX solo necesitará un puerto que lo conecte a la granja de servidores.

Por lo tanto, antes de configurar las interfaces de datos de la serie VM, debe retirar el cable de la interfaz que conecta la VPX al tráfico de la parte del cliente y conectarlo al cortafuegos para que este procese todo el tráfico entrante.

Paso 3 Configure las interfaces de datos.



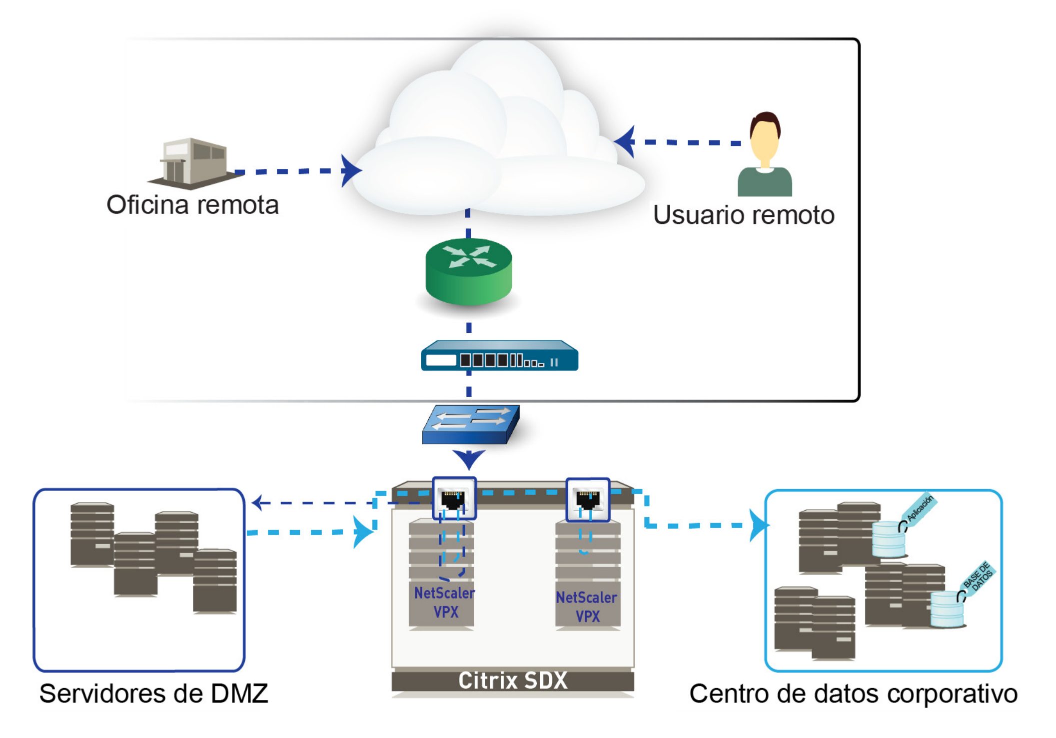
1. Inicie la interfaz web del cortafuegos.
2. Seleccione **Red > Interfaces > Ethernet**.
3. Haga clic en el enlace de una interfaz (por ejemplo, ethernet 1/1) y seleccione el **tipo de interfaz** como de **cable virtual**.
4. Haga clic en el enlace de la otra interfaz y seleccione el **tipo de interfaz** como de **cable virtual**.
5. Todas las interfaces de cable virtual deben conectarse a una zona de seguridad y un cable virtual. Para configurar estos ajustes, seleccione la ficha **Configuración** y complete las siguientes tareas:
   a. En el menú desplegable Cable virtual haga clic en **Nuevo cable virtual**, defina un **nombre**, asígnele las dos interfaces de datos (ethernet 1/1 y ethernet 1/2) y, a continuación, haga clic en **Aceptar**.
   Cuando configure ethernet 1/2, seleccione este cable virtual.
   b. Seleccione **Nueva zona** en el menú desplegable **Zona de seguridad**, defina un **nombre** para la nueva zona, por ejemplo "cliente" y, a continuación, haga clic en **Aceptar**.
6. Repita el paso 5 para la otra interfaz.
7. Haga clic en **Compilar** para guardar los cambios en el cortafuegos.

Configuración del cortafuegos de la serie VM antes de la NetScaler VPX con interfaces de cable virtual	
Paso 4 Cree una regla de política básica que permita el tráfico a través del cortafuegos. En este ejemplo se muestra cómo permitir el tráfico entre la NetScaler VPX y los servidores web. 	1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir**. 2. Asigne a la regla un nombre descriptivo en la pestaña **General**. 3. En la ficha **Origen**, establezca la **zona de origen** para la zona de la parte del cliente que ha definido. En este ejemplo, seleccione el cliente. 4. En la ficha **Destino**, establezca la **zona de destino** para la zona de la parte del servidor que ha definido. En este ejemplo, seleccione el servidor. 5. En la ficha **Aplicación**, haga clic en **Añadir** para seleccionar las aplicaciones a las que debe permitir el acceso. 6. En la pestaña **Acciones**, realice estas tareas: a. Establezca **Configuración de acción** como **Permitir**. b. Adjunte los perfiles predeterminados para la protección antivirus, antispyware y contra vulnerabilidades y para el filtrado de URL, en **Ajuste de perfil**. 7. Verifique que los logs están habilitados al final de una sesión bajo **Opciones**. Únicamente se registrará el tráfico que coincida con una regla de seguridad.

Tráfico este-oeste con el cortafuegos de la serie VM

En el siguiente ejemplo se muestra cómo implementar el cortafuegos de la serie VM para asegurar la aplicación o los servidores de la base de datos en su red. Esta situación se le aplica si dispone de dos instancias de la NetScaler VPX, una que autentica a los usuarios, termina las conexiones SSL y, a continuación, equilibra las cargas de las solicitudes en los servidores DMZ y otra que equilibra las cargas de las conexiones con los servidores corporativos que albergan la aplicación y los servidores de bases de datos en su red.

Topología antes de añadir el cortafuegos de la serie VM



Ambas instancias de la NetScaler VPX procesan la comunicación entre los servidores de DMZ y los del centro de datos corporativo. Se proporciona una nueva solicitud a la otra instancia de la NetScaler VPX, que envía la solicitud al servidor correspondiente, para el contenido que reside en el centro de datos corporativo.

Topología después de añadir el cortafuegos de la serie VM

Cuando el cortafuegos de a serie VM se implementa (este ejemplo utiliza las interfaces de capa 3), el flujo de tráfico es el siguiente:

- Todas las solicitudes entrantes se autentican y la conexión SSL se termina en la primera instancia de la NetScaler VPX. Para obtener el contenido solicitado, si reside en la DMZ, la NetScaler VPX inicia una nueva conexión al servidor. Observe que el tráfico norte-sur destinado al centro de datos corporativo o a los servidores de la DMZ lo gestiona el cortafuegos perimetral y no el cortafuegos de la serie VM.

  Por ejemplo, cuando un usuario (IP de origen 1.1.1.1) solicita contenido desde un servidor de la DMZ, la IP de destino es 20.5.5.1 (VIP de la NetScaler VPX). Entonces, la NetScaler VPX sustituye la dirección IP de destino, basada en el protocolo a la dirección IP del servidor interno, p. ej. 192.168.10.10. El tráfico de retorno desde el servidor se envía de vuelta a la NetScaler VPX en 20.5.5.1 y se envía al usuario con la dirección IP 1.1.1.1.

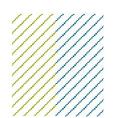
- El cortafuegos de la serie VM procesa todas las solicitudes entre los servidores de DMZ y el centro de datos corporativo. Para el contenido que reside en el centro de datos corporativo, el cortafuegos de la serie VM procesa la solicitud de forma transparente (si se implementa usando las interfaces de capa 2 o de cable virtual) o la enruta (usando las interfaces de capa 3). Entonces, se facilita a la segunda instancia de la NetScaler VPX. Esta instancia de la NetScaler VPX equilibra las cargas de la solicitud en los servidores del centro de datos corporativo, dándole así servicio. El tráfico de retorno utiliza la misma ruta que la solicitud entrante.

Por ejemplo, cuando un servidor de la DMZ (p. ej. 192.168.10.10) necesita contenido de un servidor del centro de datos corporativo (p. ej. 172.16.10.20), la dirección IP de destino es 172.168.10.3 (la VIP de la segunda NetScaler). La solicitud se envía al cortafuegos de la serie VM en 192.168.10.2, donde el cortafuegos realiza una búsqueda de política y dirige la solicitud a 172.168.10.3. Entonces, la NetScaler VPX sustituye la dirección IP de destino, basada en el protocolo, por la dirección IP del servidor interno 172.16.10.20. El tráfico de retorno procedente de 172.168.10.20 se envía entonces a la NetScaler VPX en 172.168.10.3 y la dirección IP de origen se establece como 172.168.10.3 y se dirige al cortafuegos de la serie VM en 172.168.10.2. En el cortafuegos de la serie VM, se realiza de nuevo una búsqueda de política y el tráfico se dirige al servidor de la DMZ (192.168.10.10).



Para filtrar e informar sobre la actividad de los usuarios en la red, debido a que todas las solicitudes se inician desde la NetScaler VPX, debe activar la *inserción de encabezado* de HTTP o la *opción TCP para inserción de IP* en la primera instancia de la NetScaler VPX.

Configuración del cortafuegos de la serie VM para asegurar el tráfico este-oeste		
Paso 1	Instalación del Cortafuegos de la serie VM	Si planea implementar el cortafuegos de la serie VM usando interfaces de cable virtual o de capa 2, asegúrese de habilitar el modo de capa 2 en todas las interfaces de datos en el servidor de SDX.
Paso 2	Vuelva a conectar el cable a las interfaces asignadas a la NetScaler VPX. Como la NetScaler VPX se reiniciará cuando vuelva a conectarse el cable, evalúe si desea realizar esta tarea durante una ventana de mantenimiento.	
Paso 3	Configure las interfaces de datos.	1. Seleccione **Red > Interfaces** y asigne las interfaces como tipo de capa 3 (consulte el Paso 2), capa 2 (consulte el Paso 3) o cable virtual (consulte el Paso 3).
Paso 4	Cree la política de seguridad para permitir el tráfico de aplicación entre la DMZ y el centro de datos corporativo. Zona: De DMZ a Corporativa Observe que la regla de denegación implícita denegará todo el tráfico interno de la zona excepto el que permita explícitamente la política de seguridad.	1. Haga clic en **Añadir** en la sección **Políticas > Seguridad**. 2. Asigne a la regla un nombre descriptivo en la pestaña **General**. 3. En la ficha **Origen**, establezca la **zona de origen** como DMZ y la **dirección de origen** como 192.168.10.0/24. 4. En la ficha **Destino**, establezca la **zona de destino** como Corporativa y la **dirección de destino** como 172.168.10.0/24. 5. En la ficha **Aplicación**, seleccione las aplicaciones que desea permitir. Por ejemplo, Oracle. 6. Establezca **Servicio** como **Valor predeterminado de aplicación**. 7. En la pestaña **Acciones**, establezca **Configuración de acción** como Permitir. 8. Deje el resto de opciones con los valores predeterminados. 9. Haga clic en **Compilar** para guardar los cambios.



Cortafuegos de la edición NSX de la serie VM

El cortafuegos de la edición NSX de la serie VM se ha desarrollado conjuntamente entre Palo Alto Networks y VMware. Esta solución emplea la API de NetX para integrar los cortafuegos de última generación de Palo Alto Networks y Panorama con los servidores ESXi de VMware para proporcionar una amplia visibilidad y una activación segura de aplicaciones de todo el tráfico de centros de datos, incluyendo comunicaciones con máquinas virtuales en el host.

Los siguientes temas ofrecen información sobre el cortafuegos de la edición NSX de la serie VM.

- ▲ Presentación del cortafuegos de la edición NSX de la serie VM
- ▲ Implementación del cortafuegos de la edición NSX de la serie VM

Presentación del cortafuegos de la edición NSX de la serie VM

NSX, la plataforma de redes y seguridad de VMware diseñada para el centro de datos definido por software (SDDC), ofrece la capacidad de implementar el cortafuegos de Palo Alto Networks como un servicio en los servidores ESXi. El término *SDDC* es un término de VMware que hace referencia a un centro de datos en el que una infraestructura (recursos informáticos, red y almacenamiento) se virtualizan mediante NSX de VMware.

Para mantenerse al día con los cambios del ágil SDDC, la edición NSX del cortafuegos de la serie VM simplifica el proceso de implementación de un cortafuegos de última generación de Palo Alto Networks y refuerza de forma continua la seguridad y conformidad normativa con el tráfico horizontal del SDDC. Si desea información detallada sobre la edición NSX de la serie VM, consulte los siguientes temas:

- ¿Cuáles son los componentes de la solución?
- Funcionamiento de los componentes
- Ventajas de la solución

¿Cuáles son los componentes de la solución?

Los componentes de esta solución conjunta de Palo Alto Networks y VMware son:

Proveedor	Componente	Versión mínima	Descripción
VMware	Servidor vCenter	5.5	El servidor vCenter es la herramienta de gestión centralizada de la gama vSphere.
	Administrador NSX	6.0	La plataforma Networking and Security de VMware debe instalarse y registrarse con el servidor vCenter. El administrador NSX es necesario para implementar el cortafuegos de la edición NSX de la serie VM en los hosts ESXi dentro de un clúster ESXi.
	Servidor ESXi	5.5	ESXi es un hipervisor que permite la virtualización informática.

Proveedor	Componente	Versión mínima	Descripción
Palo Alto Networks	PAN-OS	6.0	La imagen base de la serie VM (PA-VM-NSX-6.0.0.zip) que se usa para implementar el cortafuegos de la edición NSX de la serie VM es PAN-OS, versión 6.0. Los requisitos mínimos de sistema para implementar el cortafuegos de la edición NSX de la serie VM en el servidor ESXi son los siguientes: • Dos vCPU, una para el plano de gestión y la otra para el plano de datos. Puede asignar 2 o 6 vCPU adicionales para asignar un total de 2, 4 u 8 vCPU al cortafuegos; el plano de gestión solo usa una vCPU y puede asignar las vCPU adicionales al plano de datos. • 5 GB de memoria. Cualquier memoria adicional se utilizará únicamente en el plano de gestión. • Un mínimo de 40 GB de espacio de disco virtual.
	Panorama	6.0	Panorama es la herramienta de gestión centralizada de los cortafuegos de última generación de Palo Alto Networks. En esta solución, Panorama trabaja con el administrador NSX para implementar, licenciar y administrar de forma centralizada (configuración y políticas) del cortafuegos de la edición NSX de la serie VM. Panorama debe poder conectarse con el administrador NSX, el servidor vCenter, los cortafuegos de la serie VM y el servidor de actualizaciones de Palo Alto Networks. Los requisitos mínimos de sistema de Panorama son los siguientes: • Dos vCPU de ocho núcleos (2,2 GHz); utilice 3 GHz si tiene 10 o más cortafuegos • 4 GB de RAM; se recomiendan 16 GB si tiene 10 cortafuegos o más • 40 GB de espacio en disco. Para ampliar la capacidad de registro, debe añadir un disco virtual o configurar el acceso a un almacén de datos NFS. Si desea información detallada consulte la Guía del administrador de Panorama.
	Edición NSX de la serie VM	6.0	La única licencia de VM disponible en esta solución es VM-1000 en modo de hipervisor (VM-1000-HV).

Servidor vCenter

El servidor vCenter es necesario para gestionar el administrador NSX y los hosts ESXi en su centro de datos. Esta solución conjunta requiere que los hosts ESXi se organicen uno o más clústeres en el servidor vCenter y deben conectarse con un conmutador virtual distribuido.

Si desea información sobre clústeres, conmutadores virtuales distribuidos, DRS y el servidor vCenter, consulte su documentación de VMware: http://www.vmware.com/support/vcenter-server.html.

Administrador NSX

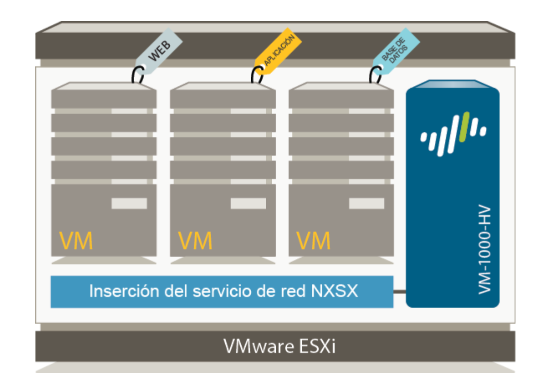
NSX es una plataforma de virtualización de red de VMware que se integra completamente con vSphere. El cortafuegos NSX y el compositor de servicios son funciones clave del administrador NSX. El cortafuegos NSX es un cortafuegos lógico que le permite vincular los servicios de red y seguridad a las máquinas virtuales, y el compositor de servicios le permite agrupar máquinas virtuales y crear políticas para redirigir el tráfico al cortafuegos de la serie VM (llamado servicio Palo Alto Networks NGFW en el administrador NSX).

Panorama

Panorama se usa para registrar la edición NSX del cortafuegos de la serie VM como servicio *Palo Alto Networks NGFW* en el administrador NSX. El registro del servicio Palo Alto Networks NGFW en el administrador NSX permite al administrador NSX implementar la edición NSX del cortafuegos de la serie VM en cada host ESXi del clúster ESXi.

Panorama sirve como punto central de administración de los cortafuegos de la edición NSX de la serie VM. Cuando se implementa un nuevo cortafuegos de la edición NSX de la serie VM, se comunica con Panorama para obtener la licencia y recibe su configuración/políticas de Panorama. Todos los elementos de configuración, políticas y grupos de direcciones dinámicas de los cortafuegos gestionados pueden gestionarse de forma centralizada en Panorama mediante grupos de dispositivos y plantillas. La integración de la API XML basada en REST de esta solución permite a Panorama sincronizarse con el administrador NSX y los cortafuegos de la edición NSX de la serie VM para permitir el uso de grupos de direcciones dinámicas y compartir el contexto entre el entorno virtualizado y la aplicación de seguridad. Para obtener más información, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

Edición NSX de la serie VM



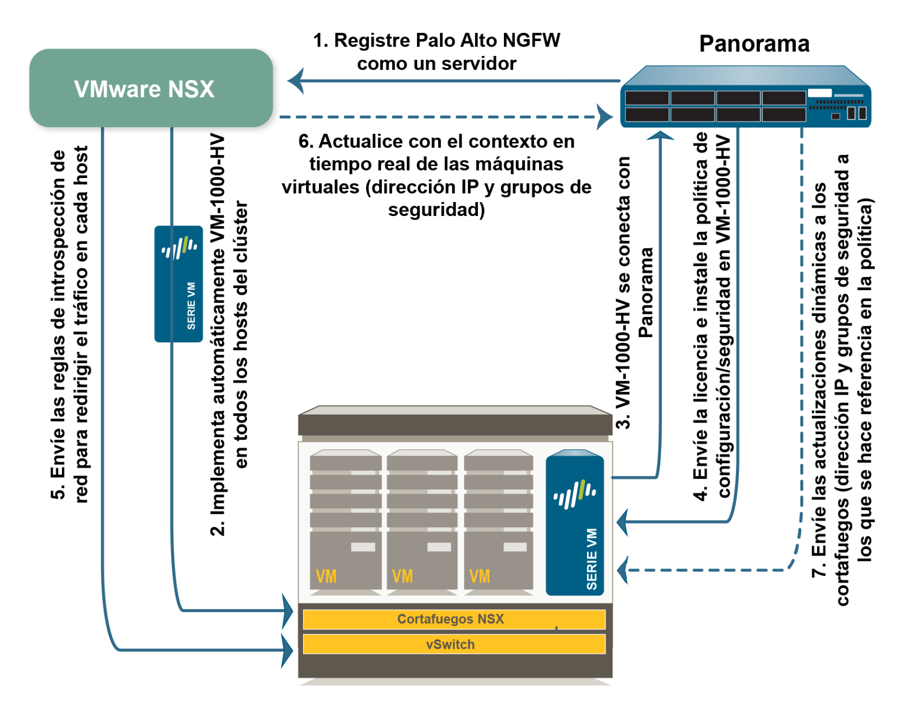
La edición NSX de la serie VM es el cortafuegos de la serie VM que se implementa en el hipervisor ESXi. La integración con la API NetX posibilita automatizar el proceso de instalar el cortafuegos de la serie VM directamente en el hipervisor ESXi y permite al hipervisor reenviar el tráfico al cortafuegos de la serie VM sin usar la configuración vSwitch; por ello, no requiere ningún cambio a la topología de red virtual.

La edición NSX de la serie VM solo admite interfaces cableadas virtuales. En esta edición Ethernet 1/1 y Ethernet 1/2 están vinculados mediante un cableado virtual y usa la API del plano de datos NetX para comunicarse con el hipervisor. Las interfaces de la capa 2 o la capa 3 no son obligatorias ni compatibles con la edición NSX de la serie VM, y por ello el cortafuegos no podrá realizar acciones de conmutación ni enrutamiento.

La única licencia disponible para esta versión del cortafuegos de la serie VM es la VM-1000-HV. Si desea un breve resumen de la capacidad, consulte Modelos de la serie VM; si desea información completa sobre las capacidades máxima admitidas en la licencia VM-1000-HV, consulte la Hoja de datos de la serie VM.

Funcionamiento de los componentes

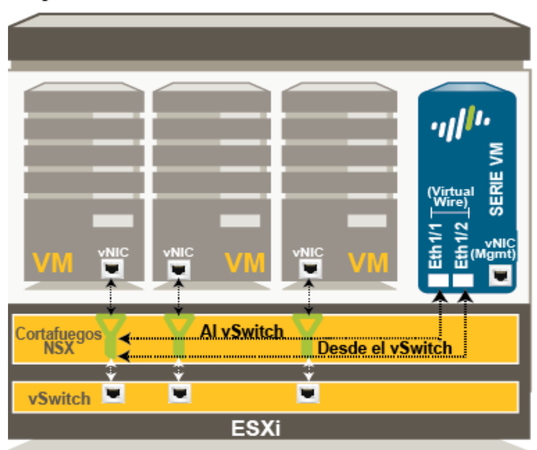
Para estar a la altura de los desafíos de seguridad del centro de datos definido por software, el administrador NSX, los servidores ESXi y Panorama trabajan en perfecta sincronía para automatizar la implementación del cortafuegos de la serie VM.



1. Registre el servicio Palo Alto Networks NGFW: El primer paso es registrar Palo Alto Networks NGFW como servicio en el administrador NSX. El proceso de registro usa la API del plano de gestión de NetX para activar la comunicación bidireccional entre Panorama y el administrador NSX. Panorama se configura con la dirección IP y las credenciales de acceso para iniciar la conexión y registrar el servicio Palo Alto Networks NGFW en el administrador NSX. La configuración incluye la URL de acceso de la imagen base de la serie VM que es obligatoria para implementar el cortafuegos de la edición NSX de la serie VM, el código de autorización para recuperar la licencia y el grupo de dispositivos al que pertenecerán los cortafuegos de la serie VM. El administrador NSX usa esta conexión con el plano de gestión para compartir actualizaciones sobre los cambios en el entorno virtual con Panorama.

2. Implemente la serie VM automáticamente desde NSX: El administrador NSX recopila la imagen base de la serie VM de la URL especificada durante el registro e instala una instancia del cortafuegos de la serie VM en cada host ESXi del clúster ESXi. A partir de un grupo de IP de gestión estáticas (que define en el administrador NSX), se asigna una dirección IP de gestión al cortafuegos de la serie VM y la dirección IP de Panorama se proporciona al cortafuegos. Cuando el cortafuegos se inicia, la API de integración del plano de datos NetX conecta el cortafuegos de la serie VM al hipervisor para que pueda recibir el tráfico desde el vSwitch.

Flujo de tráfico en la edición NSX de la serie VM



3. Establecimiento de comunicación entre el cortafuegos de la serie VM y Panorama: El cortafuegos de la serie VM inicia una conexión con Panorama para obtener su licencia. Panorama recupera la licencia del servidor de actualización y la envía al cortafuegos. El cortafuegos de la serie VM recibe la licencia (VM-1000-HV) y se reinicia con un número de serie válido.

4. Instale la configuración/política desde Panorama en el cortafuegos de la serie VM: El cortafuegos de la serie VM se vuelve a conectar con Panorama y proporciona su número de serie. Panorama ahora añade el cortafuegos al grupo de dispositivos que se definió en el proceso de registro y envía la política predeterminada al cortafuegos. El cortafuegos de la serie VM ahora está disponible como máquina virtual de seguridad que puede configurarse más detalladamente para activar con seguridad las aplicaciones en la red.

5. Envío de las reglas de redireccionamiento de tráfico desde el cortafuegos NSX: En el compositor de servicios del cortafuegos NSX puede crear grupos de seguridad y definir reglas de introspección de red que especifiquen qué invitados de qué tráfico se enviarán al cortafuegos de la serie VM. Consulte Reglas de políticas integradas para obtener información detallada.

6. Reciba actualizaciones en tiempo real desde el administrador NSX: El administrador NSX envía actualizaciones en tiempo real de los cambios en el entorno virtual a Panorama. Estas actualizaciones incluyen información sobre los grupos de seguridad y direcciones IP de invitados que forman parte del grupo de seguridad cuyo el tráfico se redirige al cortafuegos de la serie VM. Consulte Reglas de políticas integradas para obtener información detallada.

7. Uso de grupos de direcciones dinámicas en actualizaciones dinámicas de envío y políticas desde Panorama a los cortafuegos de la serie VM: En Panorama puede usar las actualizaciones en tiempo real de grupos de seguridad para crear grupos de direcciones dinámicas, vincularlas a políticas de seguridad y enviar esas políticas a los cortafuegos de la serie VM. Todos los cortafuegos de la serie VM del grupo de dispositivos tendrán el mismo conjunto de políticas, y ahora están completamente controlados para asegurar el SDDC. Consulte Instauración de políticas mediante grupos de direcciones dinámicas para obtener información detallada.

Reglas de políticas integradas

El cortafuegos NSX y el cortafuegos de la serie VM colaboran para reforzar la seguridad; cada una proporciona un conjunto de reglas de gestión de tráfico que se aplican al tráfico de cada host ESXi. El primer conjunto de reglas se define en el cortafuegos NSX; estas reglas determinan el tráfico desde el que se dirigen los invitados del clúster al cortafuegos de la serie VM. El segundo conjunto de reglas (reglas de cortafuegos de próxima generación de Palo Alto Networks) se define en Panorama y se envía a los cortafuegos de la serie VM. Estas son reglas de reforzamiento de seguridad para el tráfico que se dirige al servicio Palo Alto Networks NGFW. Estas reglas determinan cómo debe procesar el cortafuegos de la serie VM (admitir, denegar, inspeccionar y restringir) la aplicación para activarla con seguridad en su red.

- **Reglas definidas en el cortafuegos NSX**: las reglas para dirigir el tráfico desde los invitados de cada host ESXi se configuran en el administrador NSX. El compositor de servicios en el administrador NSX le permite definir el tipo de protección de seguridad, como por ejemplo las reglas de cortafuegos que se aplicarán a los invitados del clúster ESXi. Para definir las reglas del cortafuegos NSX deberá agregar en primer lugar los invitados a grupos de seguridad y después crear políticas de composición del servicio NSX para redirigir el tráfico de estos grupos de seguridad al servicio Palo Alto Networks NGFW y el cortafuegos NSX.

  El siguiente diagrama ilustra la forma en que los grupos de seguridad pueden componerse de invitados en distintos hosts ESXi de un clúster.

  Agrupación de invitados en grupos de seguridad de un clúster

  En el caso del tráfico que el cortafuegos de la serie VM debe examinar y asegurar, las políticas del compositor de servicios NSX redirigen el tráfico al servicio Palo Alto Networks NGFW. Este tráfico se dirige al cortafuegos de la serie VM, que lo procesa antes de pasarlo al conmutador virtual.

El tráfico entre grupos de seguridad se redirige al servicio Palo Alto NGFW

VM-SERIES

Controlador de dominios

VM

Web Front End

Aplicación

Base de datos

El tráfico no se redirige al servicio Palo Alto NGFW

El tráfico que el cortafuegos VM no tiene que inspeccionar, por ejemplo la copia de seguridad de datos de red de ejemplo o el tráfico hacia un controlador de dominio interno, no tiene que redirigirse al cortafuegos de la serie VM y-puede enviarse al conmutador virtual para continuar su procesamiento.

- **Reglas gestionadas centralmente en Panorama y que aplica el cortafuegos de la serie VM**: el cortafuegos de la serie VM aplica reglas de cortafuegos de última generación. Estas reglas se definen y gestionan centralmente en Panorama mediante grupos de dispositivos y plantillas y se envían a los cortafuegos de la serie VM. A continuación el cortafuegos de la serie VM refuerza la política de seguridad comparando la dirección IP de origen o destino (el uso de grupos de direcciones dinámicas para cumplimentar los miembros del grupo en tiempo real y envía el tráfico a los filtros del cortafuegos NSX).

  Para entender la forma en que el administrador NSX y Panorama se sincronizan con los cambios en SDDC y garantizar que el cortafuegos de la serie VM instaura constantemente la política, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

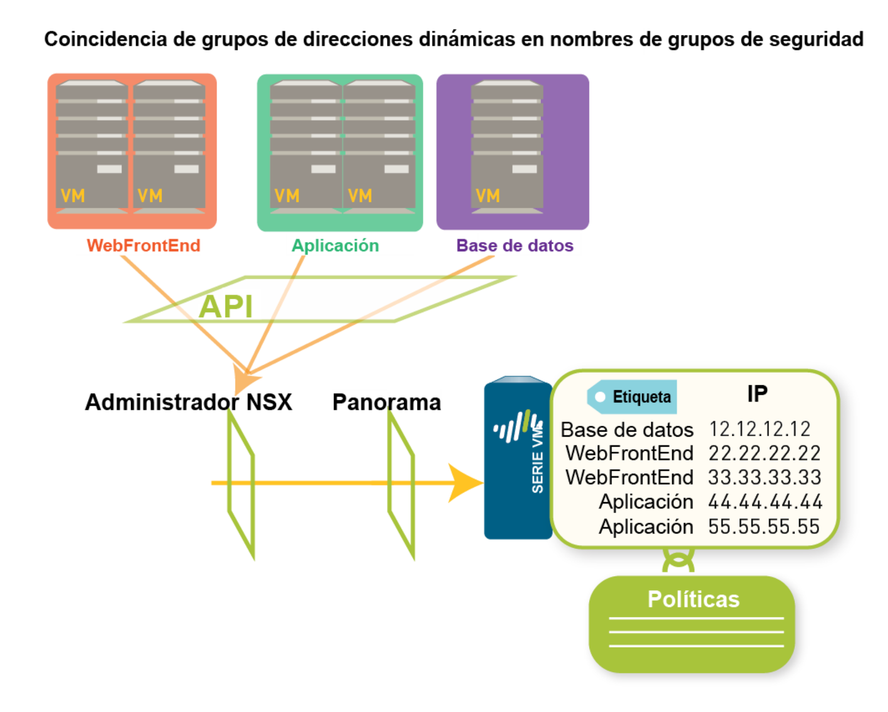
Instauración de políticas mediante grupos de direcciones dinámicas

A diferencia de otras versiones del cortafuegos de la serie VM, la edición NSX no usa zonas de seguridad como mecanismo principal de segmentación del tráfico porque ambas interfaces de cableado virtual pertenecen a la misma zona. En su lugar, la edición NSX usa grupos de direcciones dinámicas para segmentar el tráfico.

Un grupo de direcciones dinámicas se usa como objeto de recurso o destino en una política de seguridad. Como las direcciones IP cambian constantemente en un entorno de centro de datos, los grupos de direcciones dinámicas ofrecen una forma de automatizar el proceso de referencia a las direcciones de origen o destino dentro de las políticas de seguridad. A diferencia de los objetos de direcciones estáticas, que deben actualizarse manualmente en la configuración y asignarse siempre que hay un cambio de dirección (adición, eliminación o traslado), los grupos de direcciones dinámicas se adaptan automáticamente a los cambios.

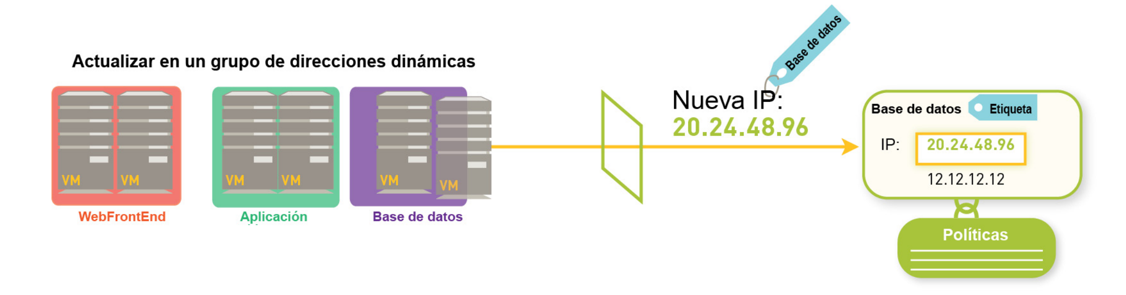
Todos los grupos de seguridad que se definen en el administrador NSX se proporcionan automáticamente como actualizaciones de Panorama mediante la integración del plano de gestión de la API de NetX, y puede usarse como criterio de filtro para crear grupos de direcciones dinámicas; el cortafuegos filtra según el nombre del grupo de seguridad, que es una etiqueta, para encontrar todos los miembros que pertenecen a un grupo de seguridad.

Por ejemplo, si tiene una arquitectura multinivel para aplicaciones web, en el administrador NSX puede crear tres grupos de seguridad para los servidores WebFrontEnd, servidores de aplicaciones y servidores de bases de datos. El administrador NSX actualiza Panorama con el nombre de los grupos de seguridad y la dirección IP de los invitados que se incluyen en cada grupo de seguridad.



En Panorama puede crear tres grupos de direcciones dinámicas para los objetos etiquetados como de base de datos, aplicación y WebFrontEnd. A continuación, en la política de seguridad puede usar los grupos de direcciones dinámicas como objeto de origen o destino, definir las aplicaciones que pueden atravesar estos servidores y enviar las reglas a los cortafuegos VM.

Cada vez que se añade o modifica un invitado en el clúster ESXi o se actualiza o crea un grupo de seguridad, el administrador NSX usa la API XML basada en REST de PAN-OS para actualizar Panorama con la dirección IP y el grupo de seguridad al que pertenece el invitado.





Para asegurar que el nombre de cada grupo de seguridad es único, el servidor vCenter asigna una Id. de referencia de objeto gestionado (MOB) al nombre que defina para el grupo de seguridad. La sintaxis empleada para mostrar el nombre de un grupo de seguridad en Panorama es *nombre_especificado-securitygroup-número*; por ejemplo, *WebFrontEnd-securitygroup-47*.

Cuando Panorama recibe la notificación de la API verifica o actualiza la dirección IP de cada invitado y el grupo de seguridad al que pertenece ese invitado. A continuación Panorama envía esas actualizaciones en tiempo real a todos los cortafuegos que se incluyen en el grupo de dispositivos y notifica a los grupos de dispositivos de la configuración del gestor de servicios de Panorama.

En cada cortafuegos todas las reglas de políticas que hacen referencia a esos grupos de direcciones dinámicas se actualizan en el momento de la ejecución. Como el cortafuegos compara la etiqueta del grupo de seguridad para determinar los miembros de un grupo de direcciones dinámicas, no tiene que modificar ni actualizar la política cuando aplique cambios en el entorno virtual. El cortafuegos compara las etiquetas para buscar los miembros actuales de cada grupo de direcciones dinámicas y aplica la política de seguridad a la dirección IP de origen/destino que se incluye en el grupo.

Ventajas de la solución

La edición NSX del cortafuegos de la serie VM se centra en asegurar las comunicaciones horizontales en el centro de datos definido por software. La implementación del cortafuegos tiene las siguientes ventajas:

- **Implementación automatizada**: el administrador NSX automatiza el proceso de distribución de los servicios de seguridad de cortafuegos de última generación y el cortafuegos VM permite una instauración transparente de la seguridad. Cuando se añade un host ESXi a un clúster, se implementa automáticamente un nuevo cortafuegos de la serie VM, que se provisionen y está disponible para la instauración inmediata de políticas sin ninguna intervención manual. El flujo de trabajo automatizado le permite estar al día con las implementaciones de máquinas virtuales de su centro de datos. El modo de hipervisor del cortafuegos elimina la necesidad de reconfigurar los puertos/vSwitch/topología de red; como cada host ESXi tiene una instancia del cortafuegos, el tráfico no debe atravesar la red ni pasar por la red de retorno para su inspección y una instauración coherente de políticas.

- **Integración más estrecha entre el entorno virtual y la instauración de la seguridad dinámica**: los grupos de direcciones dinámicas están al día de los cambios en las máquinas/aplicaciones virtuales y garantizan que la política de seguridad está sincronizada con los cambios en la red. Esta capacidad de estar al día ofrece visibilidad y protección de las aplicaciones en un entorno ágil.

- **Gestión centralizada más sólida**: los cortafuegos implementados con esta solución se licencian y gestionan con Panorama, la herramienta de gestión centralizada de Palo Alto Networks. Si usa Panorama para gestionar los cortafuegos de centros de datos y perímetros (cortafuegos virtuales y basados en hardware), podrá centralizar la gestión de políticas y mantener la agilidad y coherencia en la instauración de políticas en toda la red.

En resumen, esta solución garantiza que la naturaleza dinámica de la red virtual se asegure con una carga administrativa mínima. Puede implementar con éxito aplicaciones con una mayor velocidad, eficiencia y seguridad.

Implementación del cortafuegos de la edición NSX de la serie VM

Para implementar el cortafuegos de la edición NSX de la serie VM debe usar el siguiente flujo de trabajo:

- ❒ **Paso 1: Configuración de componentes**: para implementar la edición NSX de la serie VM, configure los siguientes componentes:
  - Configure el servidor vCenter, instale y registre el administrador NSX con el servidor vCenter.

    Si aun no ha configurado el conmutador virtual y ha agrupado los hosts ESXi en los clústeres, consulte la documentación de VMware para ver instrucciones sobre la configuración del entorno vSphere. Este documento no le lleva por el proceso de configuración de los componentes VMware de esta solución.
  - Actualice Panorama a la versión 6.0. Creación de un grupo de dispositivos y plantillas en Panorama. Si no conoce Panorama, consulte la Guía del administrador de Panorama para ver instrucciones sobre la configuración de Panorama.
  - Descargue y guarde la plantilla ovf para la edición NSX del cortafuegos VM en un servidor web. El administrador NSX debe tener acceso de red a este servidor web de modo que pueda implementar el cortafuegos de la serie VM según sea necesario. No puede alojar la plantilla ovf en Panorama.
  - Registre el código de autenticación de capacidad del cortafuegos de la edición NSX de la serie VM con su cuenta de asistencia técnica del portal de asistencia. Para obtener más información, consulte Obtención de licencia del Cortafuegos de la serie VM.
- ❒ **Paso 2: Registro**: configure Panorama para que se registre con el cortafuegos de la serie VM como servicio en el administrador NSX. Una vez registrado, el cortafuegos de la serie VM se añade a la lista de servicios de red que el administrador NSX puede implementar de forma transparente como servicio.

  También es necesaria una conexión entre Panorama y el administrador NSX para obtener licencia y configurar el cortafuegos.
- ❒ **Paso 3: Implementación de los cortafuegos** y **Creación de políticas**: instale el cortafuegos de la serie VM y cree políticas para redirigir el tráfico al cortafuegos de la serie VM y asegurarlo.
  - (En el administrador NSX) Defina el grupo de direcciones IP. Una dirección IP del rango definido se asigna a la interfaz de gestión de cada instancia del cortafuegos de la serie VM.
  - (En el administrador NSX) Implemente el cortafuegos de la serie VM. El administrador NSX implementa automáticamente una instancia del VM-1000-HV en cada host ESXi del clúster.
  - (En el administrador NSX) Configure el compositor de servicios y cree grupos de seguridad. Un grupo de seguridad reúne los invitados y aplicaciones especificados para que pueda aplicar la política al grupo.
  - (En Panorama) Aplique políticas al cortafuegos de la serie VM. En Panorama puede definir, enviar y administrar políticas centralmente en todos los cortafuegos de la serie VM. En Panorama, cree grupos de acceso dinámico para cada grupo de seguridad y haga referencia a los grupos de acceso dinámico de la política; después, envíe las políticas a los cortafuegos gestionados.

    Este mecanismo de administración centralizada le permite asegurar los invitados y aplicaciones con una intervención administrativa mínima.
  - (En el administrador NSX) Defina las reglas de introspección de red que redirigen el tráfico al cortafuegos de la serie VM.

❐ **Paso 4: Supervisión y mantenimiento de la seguridad de red**: Panorama ofrece una completa vista gráfica del tráfico de la red. Utilizando las herramientas de visibilidad en Panorama [el Centro de comando de aplicación (ACC), logs y las funciones de generación de informes] puede analizar, investigar y elaborar informes de manera central sobre toda la actividad de red, identificar áreas con un posible impacto en la seguridad y traducirlas a políticas de activación de aplicaciones seguras. Si desea más información, consulte la Guía del administrador de Panorama.

Creación de un grupo de dispositivos y plantillas en Panorama

Para poder gestionar los cortafuegos de la edición NSX y la serie VM en Panorama, los cortafuegos deben pertenecer a un grupo de dispositivos; la adición de un cortafuegos a una plantilla es opcional. Los grupos de dispositivos le permiten reunir los cortafuegos que necesitan objetos y políticas similares como una unidad lógica; la configuración se define usando las fichas **Objetos** y **Políticas** en Panorama. Las plantillas se usan para configurar los ajustes necesarios para que los cortafuegos de la serie V operen en la red; la configuración se define usando las fichas **Dispositivo** y **Red** en Panorama. Por ejemplo, puede usar plantillas para definir un acceso administrativo al cortafuegos o definir ajustes de registro o perfiles de servidor en los cortafuegos gestionados.

Si no conoce Panorama, consulte la Guía del administrador de Panorama para ver instrucciones sobre la configuración de Panorama.

Creación de un grupo de dispositivos y plantillas en Panorama		
Paso 1	Inicie sesión en la interfaz web de Panorama.	Si usa una conexión segura (https) desde un navegador web, inicie sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial. (https://<dirección IP>)
Paso 2	Añada un grupo de dispositivos.	1. Seleccione **Panorama > Grupos de dispositivos** y haga clic en **Añadir**. 2. Introduzca un **Nombre** y una **Descripción** para identificar el grupo de dispositivos. 3. Haga clic en **ACEPTAR**. Cuando los cortafuegos se hayan implementado y abastecido, se mostrarán en **Panorama > Dispositivos gestionados** y se mostrará en el grupo de dispositivos. 4. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración en ejecución en Panorama.

Creación de un grupo de dispositivos y plantillas en Panorama		
Paso 3	(Opcional) Añada una plantilla.	1. Seleccione **Panorama > Plantillas** y haga clic en **Añadir**. 2. Introduzca un **Nombre** y una **Descripción** para identificar la plantilla **Nota** Las opciones de **Modo de operación**, la casilla de verificación **Sistemas virtuales** y la casilla de verificación **Modo de deshabilitación de VPN** no se aplican al cortafuegos de la serie VM. 3. Haga clic en **ACEPTAR.** 4. Haga clic en **Compilar** y seleccione **Panorama** como **Compilar tipo** para guardar los cambios en la configuración en ejecución en Panorama.

Registro del cortafuegos de la serie VM como servicio en el administrador NSX

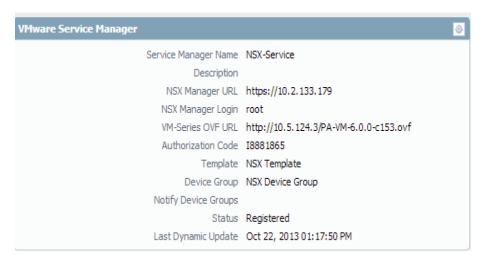
Para automatizar el abastecimiento del cortafuegos de la edición NSX de la serie VM, habilite la comunicación entre el administrador NSX y Panorama. Esta configuración se realiza una vez, y solo debe modificarse si la dirección IP del administrador NSX cambia o se supera la licencia de capacidad de implementación del cortafuegos de la serie VM.

Use Panorama para registrar el cortafuegos de la serie VM como servicio		
Paso 1	Inicie sesión en la interfaz web de Panorama.	Use una conexión segura (https) desde un navegador web para iniciar sesión usando la dirección IP y la contraseña que asignó durante la configuración inicial (https://<*dirección IP*>).
Paso 2	Configure el acceso al administrador NSX.	1. Seleccione **Panorama > Administrador de servicios VMware**. 2. Introduzca el **Nombre de dominio del servidor**. En el administrador NSX este nombre aparece en la columna Administrador de servicios en **Red y seguridad > Definiciones de servicio**. Consulte la captura de pantalla de Paso 9. 3. (Opcional) Añada una **Descripción** que identifique el cortafuegos de la serie VM como servicio. 4. Introduzca la **URL de administrador NSX** (dirección IP o FQDN) a la que accederá el administrador de NSX. 5. Introduzca las credenciales de **Inicio de sesión del administrador NSX**; nombre de usuario y contraseña, de modo que Panorama pueda autenticarse en el administrador de NSX.

Use Panorama para registrar el cortafuegos de la serie VM como servicio		
Paso 3	Especifique la ubicación del archivo OVF. Este archivo se usa para implementar cada instancia del cortafuegos.	En **URL de OVF de serie VM**, añada la ubicación del servidor web que aloja el archivo ovf. Tanto http como https son protocolos admitidos.
Paso 4 **Nota**	Adición del código de autorización. El código de autorización debe aplicarse a la versión Enterprise del modelo VM-1000-HV de la serie VM. Compruebe que la cantidad/capacidad del pedido es adecuada para admitir las necesidades de su red.	Introduzca el código de autorización que recibió con su correo electrónico de cumplimentación de pedidos. El código de autorización se usa para asignar una licencia a cada instancia de la serie VM. En el administrador NSX puede visualizar el número total de cortafuegos que está autorizado a implementar y la proporción del número de licencias que se han usado del número total de licencias que le ofrece su código de autorización.
Paso 5	Especifique el grupo de dispositivos al que pertenecen los cortafuegos y, opcionalmente, la plantilla.	Como los cortafuegos implementados en esta solución se administran centralmente desde Panorama, debe especificar el **Grupo de dispositivos** al que pertenecen los cortafuegos. Todos los cortafuegos que se implementan con el código de autorización definido en el Paso 4 pertenecen a la plantilla y el grupo de dispositivos especificados durante la implementación inicial. Si quiere reasignar los cortafuegos, debe mover manualmente el cortafuegos a una plantilla o grupo de dispositivos distinto después de su implementación.
Paso 6	Configure la notificación en distintos grupos de dispositivos a medida que aprovisione nuevas máquinas virtuales o se produzcan cambios en la red.	Si desea que los entornos virtual y de seguridad estén al día para que las políticas se apliquen de forma coherente a todo el tráfico que se dirige a los cortafuegos, deberá seleccionar el grupo de dispositivos al que hay que notificar. Seleccione los grupos de dispositivos aplicables en **Notificar grupos de dispositivos**. Los cortafuegos incluidos en los grupos de dispositivos especificados reciben una actualización en tiempo real de los grupos de dispositivos especificados reciben una actualización en tiempo real de grupos de seguridad y direcciones IP. Los cortafuegos usan esta actualización para determinar la lista más actual que constituye los grupos de direcciones dinámicas a los que se hace referencia en la política.
Paso 7	Compile los cambios realizados en Panorama.	Seleccione **Compilar** y Compilar tipo: **Panorama**.

Use Panorama para registrar el cortafuegos de la serie VM como servicio

Paso 8 Verificación del estado de conexión en Panorama



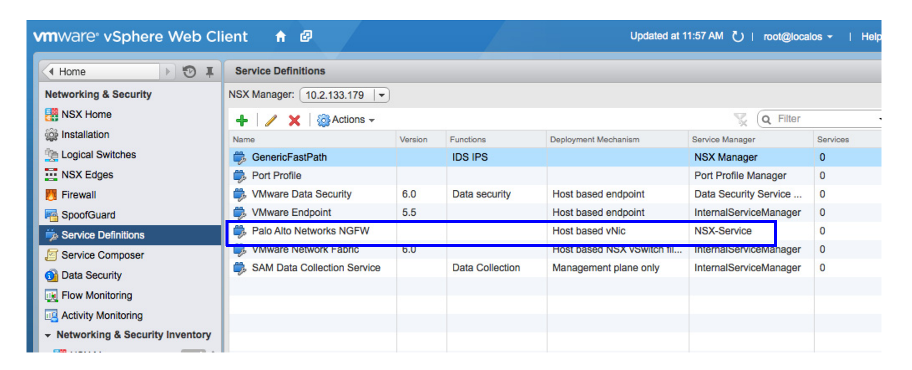
Muestra el estado de conexión entre Panorama y el administrador NSX. Cuando la conexión es correcta, el estado se muestra como **Registrado**. Esto indica que Panorama y el administrador NSX están sincronizados y el cortafuegos de la serie VM está registrado como servicio en el administrador NSX.

Los mensajes de estados de error son:

- **No conectado**: No se ha podido alcanzar/establecer una conexión de red con el administrador NSX.
- **No autorizado**: Las credenciales de acceso (nombre de usuario y/o contraseña) son incorrectas.
- **No registrado**: El servicio, administrador del servicio o perfil del servicio no está disponible o se ha eliminado en el administrador NSX.
- **Sin sincronización**: Los ajustes de configuración definidos en panorama son distintos a lo que se ha definido en el administrador NSX.
- **Sin servicio/Sin perfil de servicio**: Indica una configuración incompleta en el administrador NSX.

Paso 9 Verifique el el cortafuegos se ha registrado como un servicio en el administrador de NSX.

1. En el cliente web de vSphere, seleccione **Red y seguridad > Definiciones de servicio**.



2. Compruebe que **Palo Alto Networks NGFW** aparece en la lista de servicios disponibles para la instalación.

Implementación del cortafuegos de la serie VM

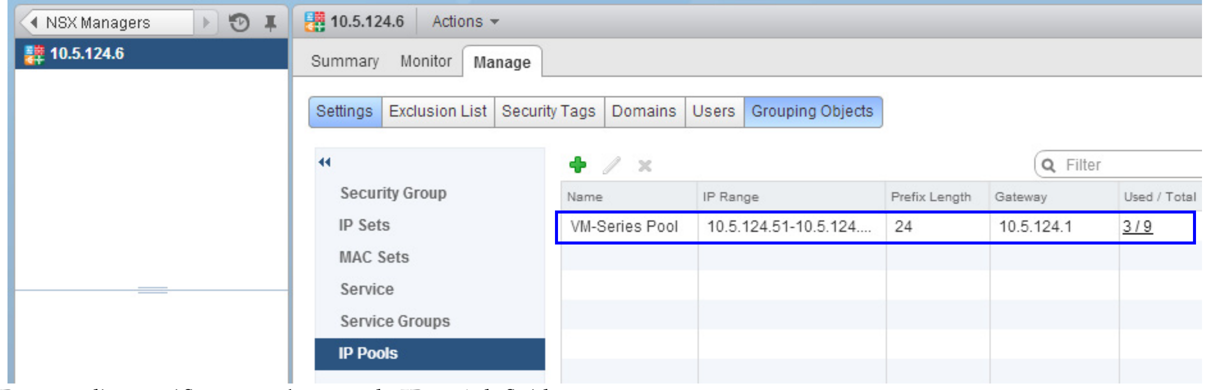
Cuando haya registrado el cortafuegos de la serie VM como un servicio (Palo Alto Networks NGFW) en el administrador de NSX, complete las siguientes tareas en el administrador de NSX.

- Definición de un grupo de direcciones IP
- Especificación de los grupos de puertos desde donde redirigir el tráfico
- Preparación del host ESXi para el cortafuegos de la serie VM
- Implementación del servicio Palo Alto Networks NGFW

Definición de un grupo de direcciones IP

El grupo de IP es un rango de direcciones IP (estáticas) que se reservan para establecer el acceso de gestión a los cortafuegos de la serie VM. Cuando el administrador NSX implementa un nuevo cortafuegos de la serie VM, la primera dirección IP disponible de este rango se asigna a la interfaz de gestión del cortafuegos.

Definición de un grupo de IP



Para añadir o verificar que el grupo de IP está definido:

1. En **Inventario de red y seguridad,** seleccione el **Administrador NSX** y haga doble clic para abrir los detalles de configuración del administrador NSX.
2. Seleccione **Gestionar > Objetos de agrupación > Grupos de IP**.
3. Haga clic en **Añadir grupo de IP** y especifique los detalles de acceso de red solicitados en la pantalla que incluye el rango de direcciones IP estáticas que quiera usar para Palo Alto Networks NGFW.

Especificación de los grupos de puertos desde donde redirigir el tráfico

Para que el administrador de NSX pueda redirigir el tráfico al cortafuegos de la serie VM, deberá seleccionar los grupos de puertos o las redes lógicas cuyo tráfico debe asegurar el cortafuegos VM.

Los grupos de puertos se definen en el perfil de servicio de Palo Alto Networks NGFW. El perfil del servicio Palo Alto Networks NGFW simplifica el proceso de implementación del cortafuegos de la serie VM; una vez configurado, el tráfico de datos del grupo de puertos seleccionado contra las políticas de seguridad NSX. Si las políticas de seguridad NSX se definen y se produce una comparación de políticas del tráfico, el tráfico se redirige al cortafuegos de la serie VM.

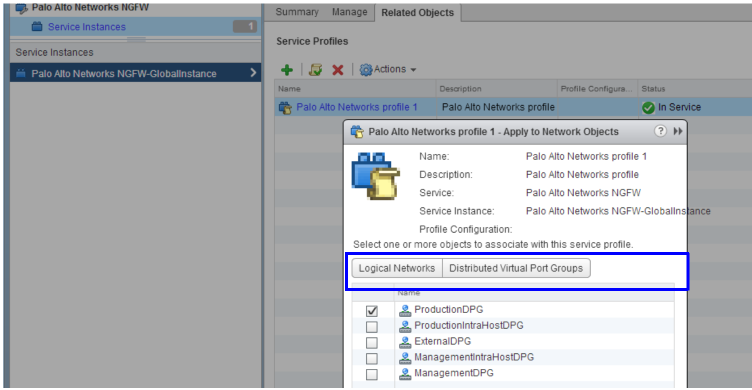
Seleccione los grupos de puertos desde desde los que se redirigirá el tráfico a Palo Alto Networks NGFW

1. Seleccione **Red y seguridad > Definiciones de servicio** y haga doble clic en el servicio **Palo Alto Networks NGFW**.
2. Haga clic en el enlace **Palo Alto NetworksNGFW-GlobalInstance** para ver el perfil de la instancia de servicio.



3. Haga clic en el vínculo **Palo Alto Networks perfil 1** y seleccione la opción **Objetos aplicados**.
4. Edite el perfil para añadir una o más **Redes lógicas** o **Grupos de puertos virtuales distribuidos** desde los que el cortafuegos recibirá el tráfico de datos.

Nota Para que el cortafuegos de la serie VM reciba tráfico del grupo de puertos seleccionado también es necesario definir las políticas de seguridad NSX que dirigen el tráfico al servicio Palo Alto NGFW. Para obtener más información, consulte Definición de políticas en el administrador NSX.



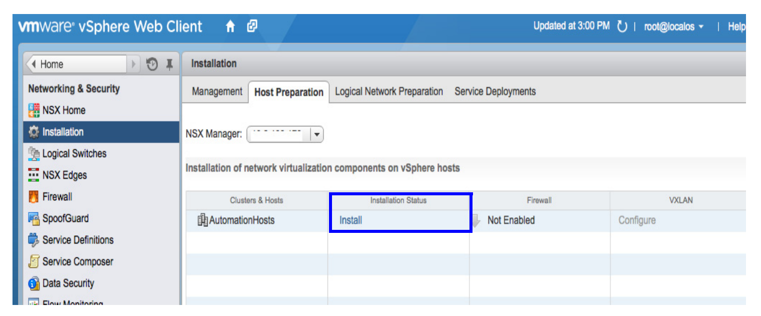
5. Haga clic en **ACEPTAR** para guardar los cambios.

Preparación del host ESXi para el cortafuegos de la serie VM

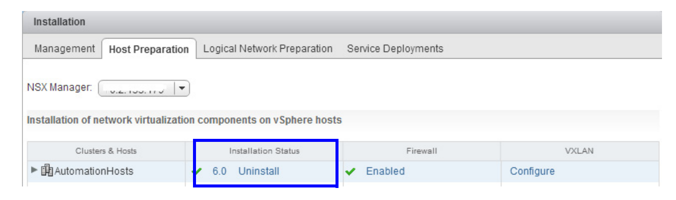
Antes de implementar el cortafuegos de la serie VM, cada invitado del clúster debe tener los componentes de NSX necesarios que permitan que el cortafuegos NSX y el de la serie VM funcionen juntos. El administrador NSX instalará los componentes (el módulo de adaptador de Ethernet .eam y el SDK) necesarios para implementar el cortafuegos de la serie VM.

Preparación de los hosts ESXi para el cortafuegos de la serie VM

1. En el administrador NSX, seleccione **Red y seguridad > Instalación > Preparación del host**.

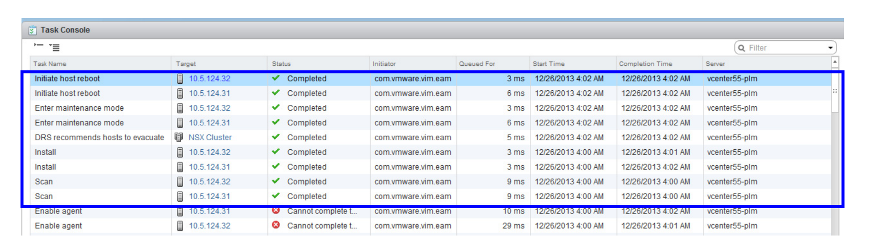


2. Haga clic en **Instalar** y verifique que el estado de instalación es correcto.



Nota Este proceso se automatiza a medida que se añaden más hosts ESXi a un clúster, y los componentes NSX necesarios se instalan automáticamente en el host ESXi.

3. Si el estado de instalación no está listo o aparece una advertencia en la pantalla, haga clic en el vínculo **Resolver**. Para supervisar el progreso del intento de reinstalación, haga clic en el vínculo **Más tareas** y consulte que las siguientes tareas se hayan completado correctamente:

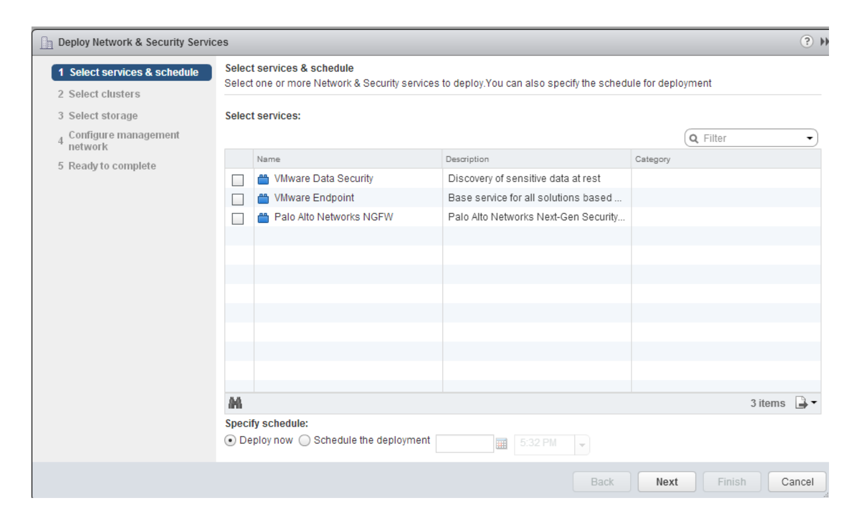


Implementación del servicio Palo Alto Networks NGFW

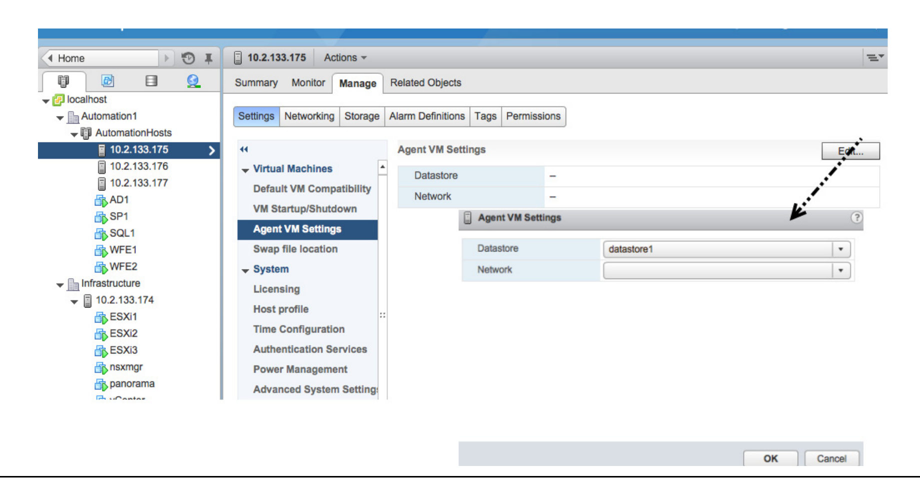
Realice los siguientes pasos para automatizar el proceso de implementación de una instancia del cortafuegos de la edición NSX de la serie VM en cada host ESXi del clúster especificado.

Implementación del servicio Palo Alto Networks NGFW

1. Seleccione **Red y seguridad > Instalación > Implementaciones de servicio**.
2. Haga clic en **Nueva implementación de servicio** (icono de signo más verde) y seleccione el servicio **Palo Alto Networks NGFW**. Haga clic en **Siguiente**.

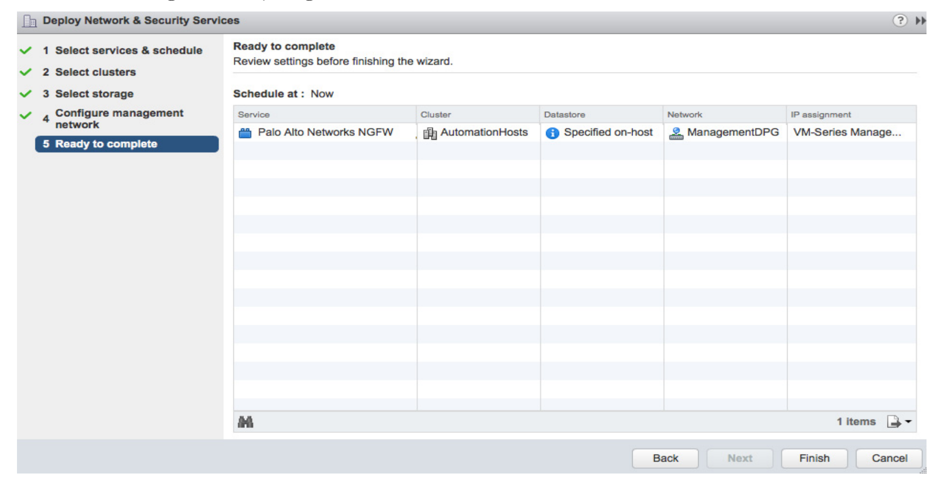


3. Seleccione el **Centro de datos** y los clústeres en los que se implementará el servicio. Una instancia del cortafuegos se implementará en cada host del clúster seleccionado.
4. Seleccione el almacén de datos en el que asignar espacio de disco para el cortafuegos. Seleccione una de las siguientes opciones según su implementación:
   - Si ha asignado un almacenamiento compartido al clúster, seleccione un almacén de datos compartido que esté disponible.
   - Si no ha asignado un almacenamiento compartido al clúster, seleccione la opción **Especificado en el host**. Asegúrese de seleccionar el almacenamiento cada host ESXi del clúster. Seleccione además la red que se usará para el tráfico de gestión en el cortafuegos de la serie VM.

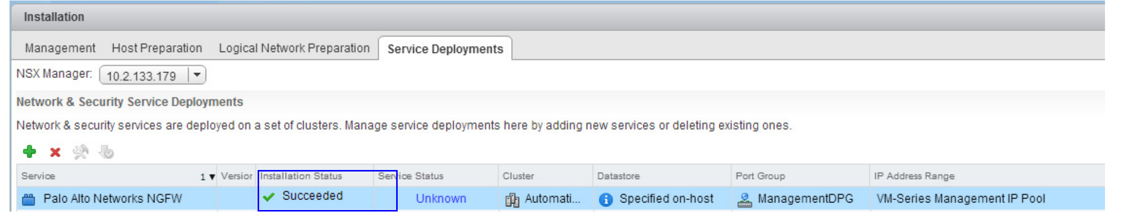


Implementación del servicio Palo Alto Networks NGFW

5. Seleccione el grupo de puertos que proporciona acceso de tráfico de red de gestión al cortafuegos.
6. Seleccione el grupo de direcciones IP desde el que asignar una dirección IP de gestión a cada cortafuegos cuando se implementa.
7. Revise su configuración y haga clic en **Finalizar**.

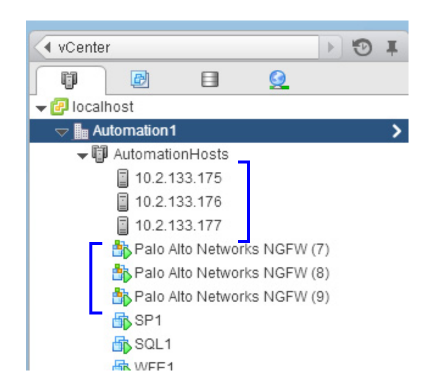


8. Compruebe que el administrador NSX comunica que el **Estado de instalación** es **Correcto**. Este proceso puede tardar un tiempo, haga clic en el vínculo **Más tareas** en vCenter para supervisar el progreso de la instalación.



Nota Si la instalación de una serie VM falla, el mensaje de error se mostrará en la columna Estado de instalación. También puede usar la ficha **Tareas** y el **Explorador de registros** en el administrador NSX para ver los detalles del fallo y consultar la documentación de VMware para conocer los pasos de resolución de problemas.

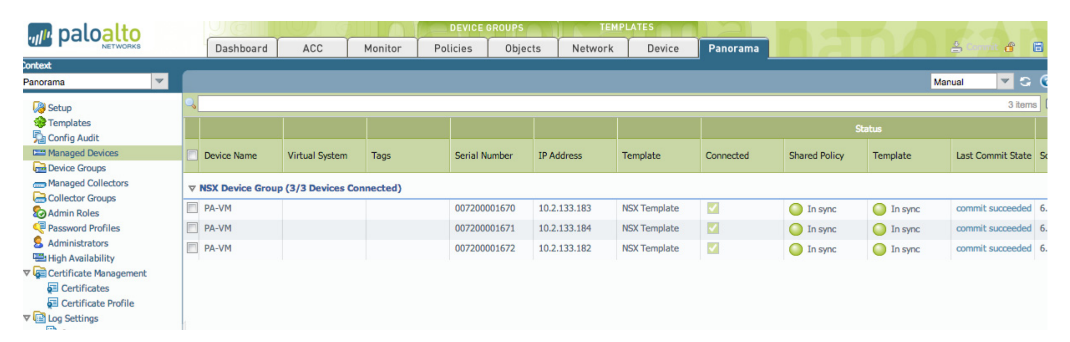
9. Compruebe que el cortafuegos se ha implementado con éxito y está conectado a Panorama.
En el servidor vCenter, seleccione **Hosts y clústeres** para comprobar que todos los hosts del clúster tienen una instancia del cortafuegos.



Implementación del servicio Palo Alto Networks NGFW

10. Acceda a la interfaz web de Panorama para asegurarse de que los cortafuegos de la serie VM están conectados y sincronizados con Panorama.

   a. Seleccione **Panorama > Dispositivos gestionados** para comprobar que los cortafuegos están conectados y sincronizados.

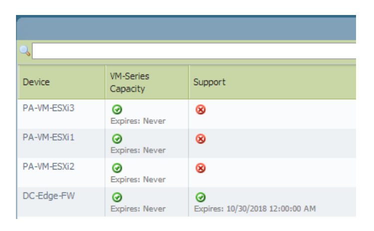


   b. Haga clic en **Compilar** y seleccione Compilar tipo como **Panorama**.

Nota Es necesario compilar Panorama periódicamente para garantizar que Panorama guarda los números de serie de dispositivos en la configuración. Si reinicia Panorama sin compilar los cambios, los dispositivos gestionados no se conectarán de nuevo con Panorama; aunque el grupo de dispositivos aparecerá en la lista de dispositivos, los dispositivos no aparecerán en **Panorama > Dispositivos gestionados**.

11. Compruebe que se ha aplicado la licencia de capacidad y cualquier licencia adicional que haya adquirido. Como mínimo debe activar la licencia de asistencia técnica en cada cortafuegos.

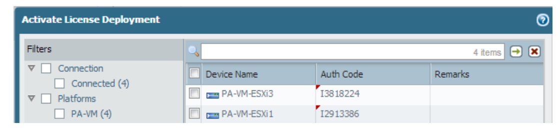
   a. Seleccione **Panorama > Implementaciones de servicio > Licencias** para comprobar que la licencia de capacidad de la serie VM se aplique.



   b. Para aplicar licencias adicionales a los cortafuegos de la serie VM:

      1. Haga clic en **Activar** en **Panorama > Implementación de dispositivos > Licencias**.

      2. Busque o filtre el cortafuegos y, en la columna **Código de autenticación**, introduzca el código de autorización de la licencia a activar. Solo es posible introducir un código de autorización una vez para cada cortafuegos



      3. Haga clic en **Activar** y compruebe que la activación de la licencia se realizó con éxito.

Creación de políticas

Los siguientes temas describen cómo crear políticas en el administrador NSX para redirigir el tráfico al cortafuegos de la serie VM y cómo crear políticas en Panorama y aplicarlas en el cortafuegos de la serie VM para que este pueda instaurar la política en el tráfico que se le redirige.

▲ Definición de políticas en el administrador NSX

▲ Aplicación de políticas al cortafuegos de la serie VM

Definición de políticas en el administrador NSX

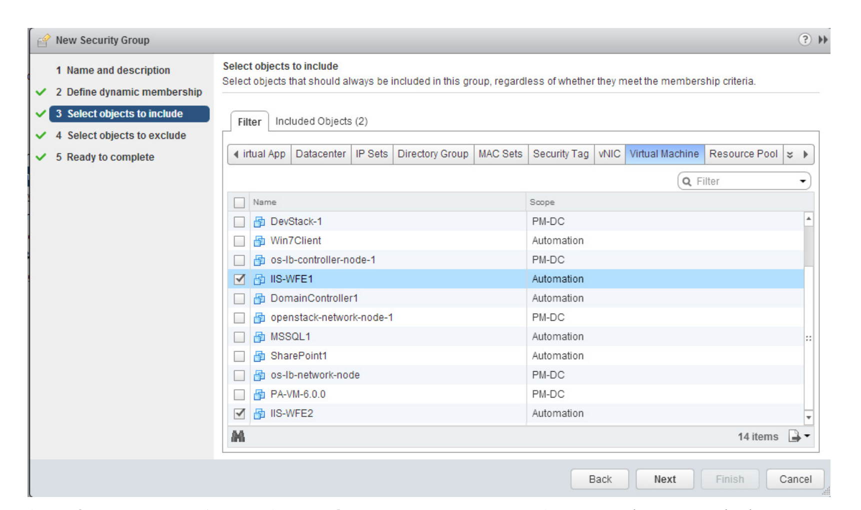
Para que el cortafuegos de la serie VM asegure el tráfico, primero debe crear grupos de seguridad en el administrador NSX y asignar máquinas virtuales (invitadas) a los grupos. Después defina y aplique reglas para redirigir el tráfico desde los hosts ESXi de estos grupos al cortafuegos de la serie VM.

Un grupo de seguridad es un contenedor lógico que reúne invitados en múltiples hosts ESXi del clúster. La creación de los grupos de seguridad facilita la gestión de los invitados y su seguridad; para comprender cómo los grupos de seguridad permiten la instauración de políticas, consulte Instauración de políticas mediante grupos de direcciones dinámicas.

Configuración de grupos de seguridad en el administrador NSX

❑ Asigne los invitados a grupos de seguridad en NSX.

1. Seleccione **Redes y seguridad > Compositor de servicios > Grupos de seguridad** y agregue un **Nuevo grupo de seguridad**.
2. Añada un **nombre** y una **descripción**. Este nombre aparecerá en la lista de criterios de coincidencia cuando defina los grupos de direcciones dinámicas en Panorama.
3. Seleccione los invitados que constituyen el grupo de seguridad. Puede añadir miembros dinámicamente usando **Definir afiliación dinámica** o estáticamente mediante **Seleccionar los objetos a incluir**. En la siguiente captura de pantalla, los invitados que pertenecen al grupo de seguridad se seleccionan con las opciones **Seleccionar los objetos a incluir** > **Máquina virtual**.

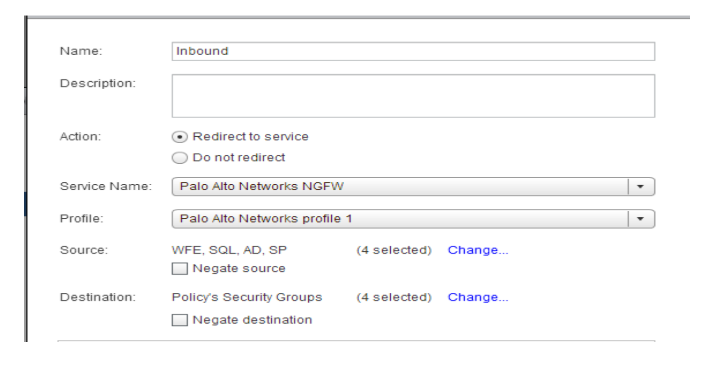


4. Revise la información y haga clic en **Aceptar** para crear el grupo de seguridad.

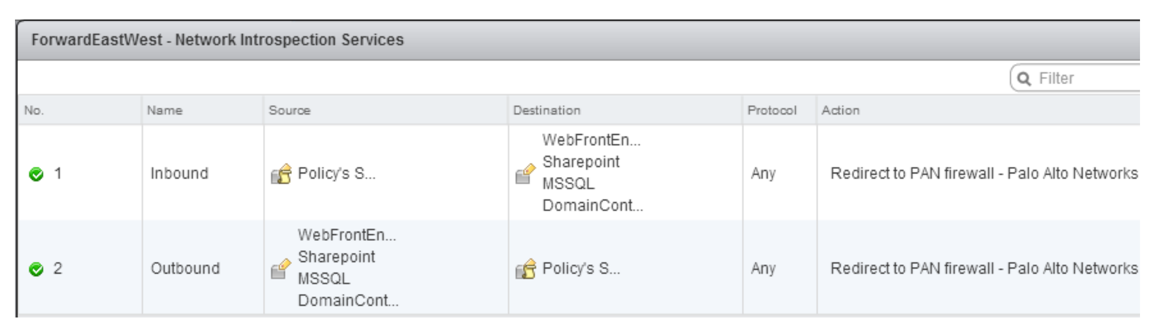
Definición de las políticas para redirigir el tráfico al cortafuegos de la serie VM

- [ ] Cree políticas de seguridad para dirigir el tráfico desde el administrador NSX al cortafuegos de la serie VM.

1. Seleccione **Redes y seguridad > Compositor de servicios > Políticas de seguridad** y haga clic en **Crear política de seguridad**.
2. Añada un **Nombre** y una **Descripción**.
3. En **Servicios de introspección de redes**, haga clic en **Añadir** e introduzca un **Nombre** para el servicio.
4. Defina la **Acción** como **Redirigir al servicio** y defina el **Nombre de servicio** como **Palo Alto NFGW**.
5. Seleccione el perfil de servicio que creó anteriormente; **Palo Alto Networks perfil 1** en este flujo de trabajo**.** Este perfil especifica los grupos de puertos y redes desde los que el cortafuegos recibe tráfico de datos. Ejecutará servicios de introspección de redes en el puerto especificado en el perfil.
6. Use el vínculo **Cambiar** bajo **Origen** y **Destino** para especificar la dirección del flujo de tráfico que requiere la introspección de la red. La selección de destino o de origen (o ambos) debe ser **Grupos de seguridad de la política**, donde podrá seleccionar los grupos de seguridad que definió antes.



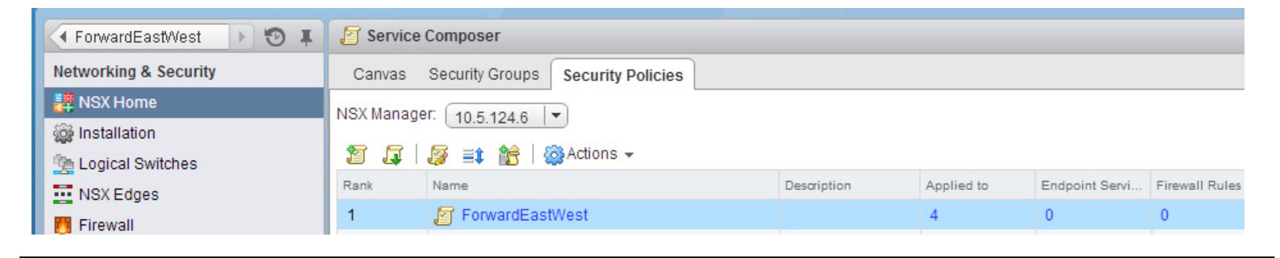
Si, por ejemplo, desea inspeccionar todo el tráfico entrante desde los grupos de seguridad a los servidores front-end web y todo el tráfico saliente de los servidores a los grupos de seguridad, la regla sería como sigue:



ForwardEastWest - Network Introspection Services

No.	Name	Source	Destination	Protocol	Action
1	Inbound	Policy's S...	WebFrontEn... Sharepoint MSSQL DomainCont...	Any	Redirect to PAN firewall - Palo Alto Networks
2	Outbound	WebFrontEn... Sharepoint MSSQL DomainCont...	Policy's S...	Any	Redirect to PAN firewall - Palo Alto Networks

La política de seguridad completa sería así:



No aplique las políticas de redireccionamiento de tráfico que creó anteriormente a no ser que comprenda el funcionamiento de las reglas en el administrador NSX, así como en el cortafuegos de la serie VM y Panorama. La política predeterminada en el cortafuegos de la serie VM se define como *denegar todo* el tráfico, lo que significa que todo el tráfico que se redirija al cortafuegos de la serie VM será descartado. Para crear políticas en Panorama y enviarlas al cortafuegos de la serie VM consulte Aplicación de políticas al cortafuegos de la serie VM. Para aplicar las políticas de redireccionamiento, consulte Aplicación de políticas de seguridad en el administrador NSX.

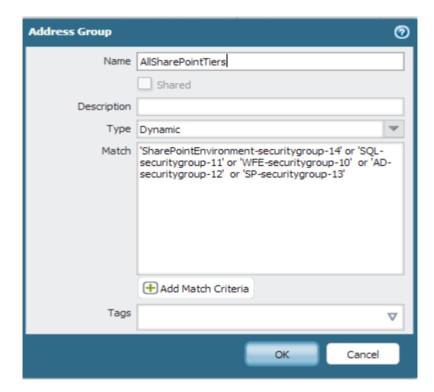
Aplicación de políticas al cortafuegos de la serie VM

Ahora que ha creado las políticas de seguridad en el administrador NSX, los nombres de los grupos de seguridad a los que se hace referencia en la política de seguridad estarán disponibles en Panorama. Ahora puede usar Panorama para administrar centralmente políticas en los cortafuegos de la serie VM.

Para gestionar una política centralizada, primero debe crear un grupo de direcciones dinámicas que coincida con el nombre de los grupos de direcciones dinámicas que coincidan con los grupos de seguridad que defina en el administrador NSX. Después, adjuntará el grupo de direcciones dinámicas como una dirección de origen o destino en la política de seguridad y lo enviará a los cortafuegos; los cortafuegos puede recuperar dinámicamente las direcciones IP de las máquinas virtuales que se incluyen en cada grupo de seguridad para garantizar que el tráfico que se origina o se dirige a las máquinas virtuales del grupo especificado cumple los requisitos.

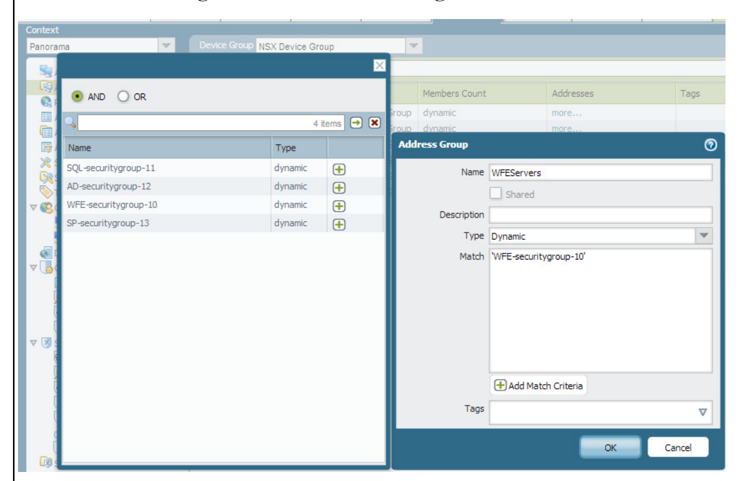
Definición de políticas en Panorama

Paso 1 Creación de grupos de direcciones dinámicas.



1. Inicie sesión en la interfaz web de Panorama.
2. Seleccione **Objeto > Grupos de direcciones**.
3. Seleccione el **Grupo de dispositivos** que creó para gestionar los cortafuegos de la edición NSX de la serie VM en Creación de un grupo de dispositivos y plantillas en Panorama.
4. Haga clic en **Añadir** e introduzca un **Nombre** y una **Descripción** para el grupo de direcciones.
5. Defina el **Tipo** como **Dinámico**.
6. Haga clic en **Añadir criterios de coincidencia**. Seleccione el operador **Y** u **O** y seleccione junto al nombre del grupo de seguridad que desea comparar.

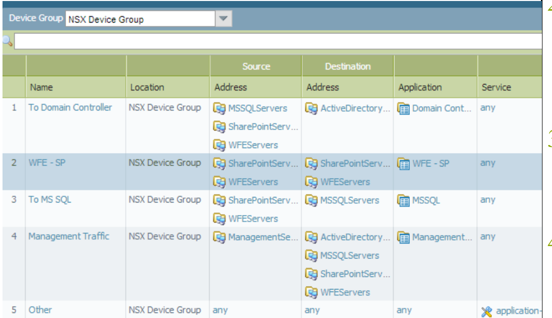
Nota Los grupos de seguridad que aparecen en los criterios de coincidencia derivan de los grupos que definió en el compositor de servicios en el administrador de NSX. Aquí solo están disponibles los grupos de seguridad a los que se hace referencia en las políticas de seguridad y desde los que se redirige el tráfico al cortafuegos de la serie VM.



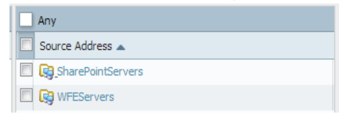
7. Haga clic en **ACEPTAR**.
8. Repita los pasos 4-7 para crear el número adecuado de Grupos de direcciones dinámicas para su red.
9. Haga clic en **Confirmar**.

Definición de políticas en Panorama

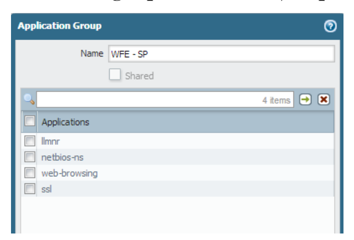
Paso 2 Cree políticas de seguridad.



1. Seleccione **Políticas > Seguridad**.
2. Seleccione el **Grupo de dispositivos** que creó para gestionar los cortafuegos de la edición NSX de la serie VM en Creación de un grupo de dispositivos y plantillas en Panorama.
3. Haga clic en **Añadir** e introduzca un **Nombre** y una **Descripción** para la regla. En este ejemplo la regla de seguridad permite todo el tráfico entre los servidores WebFrontEnd y de aplicaciones.
4. En **Dirección de origen** y **Dirección de destino**, seleccione o escriba una dirección, grupo de direcciones o región. En este ejemplo, seleccionamos un grupo de direcciones, el grupo de direcciones dinámico que creó en el Paso 1 anterior.



5. Seleccione la **Aplicación** a permitir. En este ejemplo hemos creado un **Grupo de aplicaciones** que incluye un grupo estático de aplicaciones específicas que se agrupan juntas.
   a. Haga clic en **Añadir** y seleccione **Nuevo grupo de aplicaciones**.
   b. Haga clic en **Añadir** para seleccionar la aplicación que desea añadir al grupo. En este ejemplo seleccionamos lo siguiente:

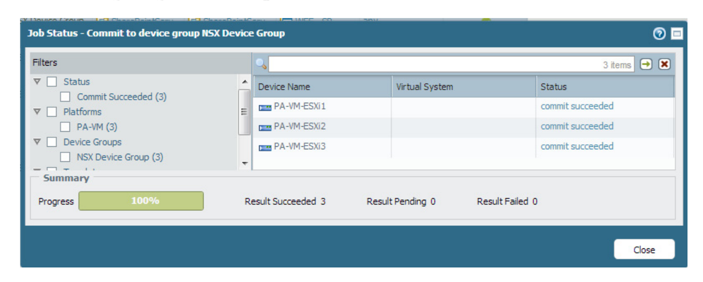


   c. Haga clic en **ACEPTAR** para crear el grupo de aplicaciones.
6. Especifique la acción (**Permitir** o **Denegar**) para el tráfico y, opcionalmente, adjunte los perfiles de seguridad predeterminados para los antivirus, anti-spyware y protección contra vulnerabilidades en **Perfiles.**
7. Repita los pasos 3- 6 anterior para crear las reglas de políticas pertinentes.
8. Haga clic en **Compilar** y seleccione Compilar tipo como **Panorama**. Haga clic en **ACEPTAR**.

Definición de políticas en Panorama

Paso 3 Aplique las políticas a los cortafuegos de la edición NSX de la serie VM.

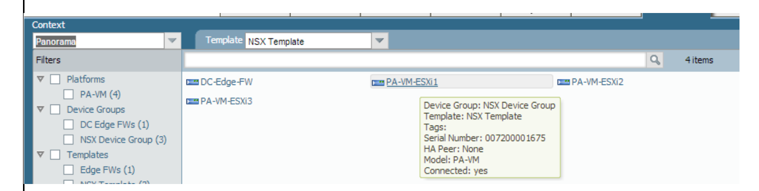
1. Haga clic en **Compilar** y seleccione Compilar tipo como **Grupos de dispositivos**.
2. Seleccione el grupo de dispositivos, que en este ejemplo es Grupo de dispositivos NSX, y haga clic en **Aceptar**.
3. Verifique que la compilación se realiza correctamente.



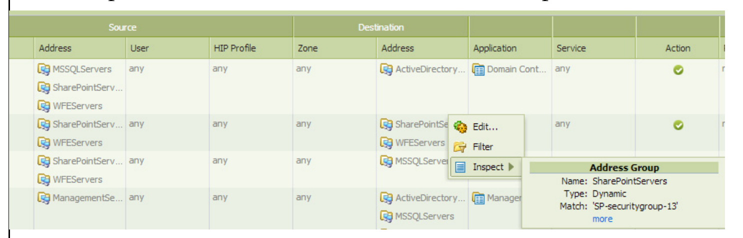
Paso 4 Valide que los miembros del grupo de direcciones dinámicas se cumplimentan en el cortafuegos de la serie VM.

Nota No puede verificar los miembros (direcciones IP registradas) del grupo de direcciones dinámicas en Panorama. Esta información solo puede verse en el cortafuegos de la serie VM que instaura la política.

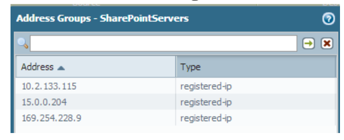
1. En Panorama, cambie el contexto del dispositivo para iniciar la interfaz web del cortafuegos al que envió las políticas.



2. En el cortafuegos de la serie VM, seleccione **Políticas > Seguridad** y seleccione una regla.
3. Seleccione la flecha desplegable junto al vínculo del grupo de direcciones y seleccione **Inspeccionar**. También puede comprobar si los criterios de coincidencia son precisos.



4. Haga clic en el vínculo **más** y compruebe que se muestra la lista de direcciones IP registradas.



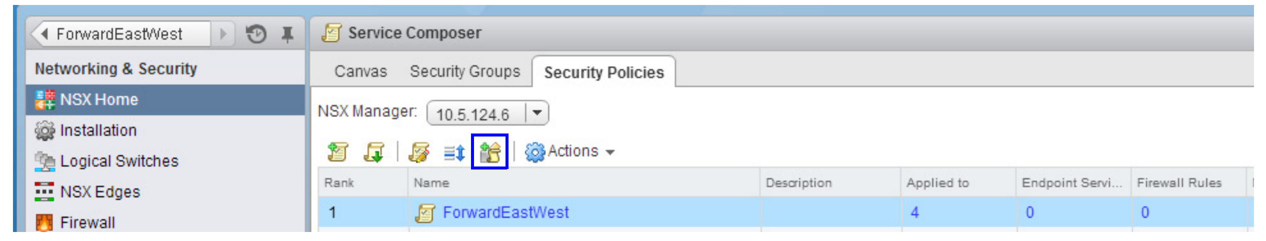
La política entra en vigor para todas las direcciones IP que pertenecen a este grupo de direcciones y se muestra aquí.

Definición de políticas en Panorama	
Paso 5 (Opcional) Use la plantilla para enviar una configuración base para la configuración de red y dispositivo, como por ejemplo servidor DNS, servidor NTP, servidor Syslog y pancarta de inicio de sesión.	Si desea más información sobre el uso de plantillas, consulte la Guía del administrador de Panorama.

❒ El último paso del proceso de implementación del cortafuegos de la edición NSX de la serie VM es aplicar las políticas de redireccionamiento a los grupos de seguridad del administrador NSX.

Aplicación de políticas de seguridad en el administrador NSX

1. Seleccione **Red y seguridad > Compositor de servicios > Políticas de seguridad**.



2. Seleccione la política de seguridad, haga clic en **Aplicar política de seguridad** y seleccione los grupos de seguridad a los que se enviarán las reglas. Las reglas se aplican a cada host ESXi que se incluye en los grupos de seguridad seleccionados.